CYBER SECURITY

Effective Practices for the establishment and maintenance of adequate cyber security at Non-Power (Research and Test) Reactor facilities

NOTICE:

The focus of this document is only on how to protect existing and future operational, security and safety systems employing digital technologies from cyber-based threats

This document is not intended to infer acceptability of methods, processes, practices, et cetera. for meeting NRC regulatory requirements or technical specifications related to reactor safety and control systems

Contents

Contents

Section 1: Executive Summary

Based on the commitments made in the U.S. Nuclear Regulatory Commission (NRC) Cyber Security Roadmap (SECY-12-0088)[1], in 2011, the staff initiated a review of cyber security programs at Research and Test Reactors, also known as NPRs, Non-Power Reactors, to determine whether regulatory action (including the establishment of cyber security requirements) was also necessary for licensed NPRs (e.g., the facilities using reactors for research, training, and testing, and to produce radioisotopes for medical, industrial, and academic applications). To determine whether regulatory action was needed, in 2012, the NRC formed a working group that included representation from the National Organization of Test, Research, and Training Reactors (TRTR) to accomplish the following:

- Gather information concerning the cyber security protections currently in place at NPR facilities.
- Conduct surveys of the participating NPR facilities to validate the information provided in the self-assessments and to evaluate the cyber security protections currently in place to protect critical digital assets.
- Analyze the information provided in the self-assessments and observations made during the site surveys within the framework of the risk posed to public health and safety from potential radiation exposure or theft of the nuclear material from the evaluated NPR facilities.

Based on the working group's analysis, the group concluded that the cyber security protections currently in place at the four NPR facilities surveyed (which are representative of the industry as a whole) were adequate based on the assessed risk, current threats/threat actors, and their existing physical security programs. This conclusion also derived from the observed minimal use, by NPR licensees, of cyber-vulnerable digital technologies in reactor safety and control functions.

The working group also noted differences between the cyber security practices and approaches used at the various facilities. Some facilities/licensees had more effective cyber security practices in various areas of their operations than other licensees. Some of this is due to the varying policies regarding cyber security at

[1] Agencywide Documents Access and Management System Accession No. (ADAMS) ML12135A050

the universities. In light of these differences, and the inevitable eventual need to upgrade and/or replace existing instrumentation, control, automation, and even physical security and emergency planning technologies, the working group recommended the development of this “effective practices” document.

This document provides a consolidation of the effective practices identified among the NPR licensees and also provides guidance for the future to ensure that NPR licensees understand the cyber security issues and consequences (and how to remain cyber-secure) as they migrate onto modern digital platforms and integrate more digital assets into their operations.

Section 2: Overview and Purpose

The purpose of this document is both to document and share effective practices for establishing and maintaining effective cyber security at NPR licensee's facilities and to provide NPR licensees with applicable guidance for the evaluation, planning, and undertaking of activities that involve the addition of, integration of, and/or the conversion to digital technologies.

One of the goals of the NRC team efforts in reviewing the current cyber security postures of the NPR licensees was to identify potential cyber weaknesses that might need to be addressed, as well as effective practices that could be shared with all licensees. The effective practices that were identified are described in the following sections of this document. Likewise the weaknesses identified in current practices are also enumerated, generally as a counterpoint to an identified effective practice that would eliminate or correct the associated weakness. The objective in documenting effective cyber security practices is not to impose new requirements and regulations on licensees, but rather to identify approaches that have been taken by NPR licensees that resulted in creating an adequate and effective cyber security environment.

During the NRC team's survey of the NPR licensees, it was noted that even though several have already made limited use of smart (digital) technologies and digital networking in their control rooms and reactor facilities, all of these licensees were looking for guidance from the NRC in regards to what would be considered as acceptable/safe (and cyber secure) uses of digital technology and what would not. This document will attempt to provide effective practices for addressing cyber security issues.

Today, even a one-for-one replacement of an analog device with an equivalent digital one can create potentially exploitable cyber vulnerabilities because the digital equivalent often incorporates additional capabilities (e.g., wireless network communications support) that were not present, or even possible, with the analog device. Thus even a seemingly simple swap out (for example changes made under 10 CFR 50.59) of an obsolete device (see Table 2.1 below) requires some thought and planning to avoid creating an adverse impact on cyber security and introducing exploitable cyber vulnerabilities. Table 2.1 shows two examples of conventional analog instruments and potential replacement devices that are digital (microprocessor based). Although the replacement smart instruments can accept the same process interfaces (I/O signals) and perform the same functions as the analog devices they replace, they also usually come with a range of additional capabilities (red text) and potentially exploitable cyber vulnerabilities.

Analog instrument		Digital Equivalent	
Chart recorder	Attributes	Trend recorder	Attributes
	Eight 4-20 mA inputs Adjustable scale and zero offset ('trim pots')		Eight 4-20 mA inputs Ethernet MODBUS/TCP Eight contact outputs Programmable trip-points Configurable plot scaling USB Bulk memory storage Menu-based configuration
PID controller	Attributes	PID controller	Attributes
	4-20 mA input 4-20 mA output PID only Local (manual dial) setpoint Local ('trim-pots') loop tuning		4-20 mA input 4-20 mA output HART communications Configurable for P,PI,PID, error-squared or R+B Remote setpoint via HART Remote loop tuning via HART

Table 2.1 – Comparing legacy analog and equivalent digital devices

The steps required to avoid an adverse cyber security impact may be as simple as physically disabling unnecessary interfaces, using configuration settings to disable undesirable features or merely providing some form of physical measure (e.g., a locked enclosure with key management procedures) to limit access to only personnel authorized to operate, service, or administer the device.

The NRC also recognizes that eventually the NPR licensees will be forced to migrate onto modern digital platforms (computer hardware, operating systems, networks, etc.) for the operation and protection of their reactors, just as they already have for the implementation of the mandated (as well as voluntary) physical security measures for their facilities. The use of modern digital platforms will open up a wide range of potential capabilities and features that were not possible with the use of conventional analog instrumentation and controls (as well as introducing potential cyber vulnerabilities). This document includes a discussion of such additional capabilities and the ways in which they may be (or should not be) used to maintain adequate cyber security.

Section 3: The requirement for adequate cyber security

The U.S. Government, and in particular the Department of Homeland Security and the intelligence community, have identified a range of threat actors (primarily foreign) who pose a real risk to the security of the United States and who have the resources and capabilities to stage and execute both physical and cyber attacks on our critical infrastructure. Nuclear reactors have been specifically identified as potential targets because of the possibility of either creating a radiological core melt-down event that would harm a large number of people and the environment, or the theft of nuclear materials that could be used to create a “dirty” bomb. Either of those outcomes would also seriously terrorize the populace and have a devastating impact on the U.S. (and even international) nuclear industry.

Although the majority of NPRs do not generally have the power level (or source term) that would enable creating a significant radiological event, they do contain highly radioactive materials that would be attractive to some terrorist groups. In addition, if an NPR were operated maliciously, with reactor safety and control systems being overridden, it might still be possible to produce an event with noticeable consequences.

For these reasons, and in accordance with Section 104 of the Atomic Energy Act, the commission (NRC) is obliged to ensure that NPR licensees establish and maintain adequate physical and cyber security over their facilities and associated digital assets to promote the common defense and security and protect public health.

Section 4: The cyber assets that require protection

The primary concern of the NRC is to ensure that a cyber attack or cyber incident cannot adversely affect the health and safety of the public or the common defense of the nation through radiological sabotage or result in the theft or diversion of nuclear materials or in the unauthorized disclosure of Safeguards Information (SGI). To that end, the NPR facility functions/activities that are of concern to the NRC, in regard to providing adequate cyber security, include the following:

Functions/Activities of Concern
Physical security of the NPR facility
Detection of unsafe/unauthorized conditions
Personnel access monitoring and control
Reactor safety
Reactor operational control
Emergency response/communications
Storage and protection of SGI
Accurate inventory/location of nuclear materials

Table 4.1 – Critical NPR functions requiring adequate cyber security

Physical Protection of digital assets - Digital systems and devices that are used to perform or support the functions listed in Table 4.1 (also called "critical digital assets" or "CDAs") need adequate protection against cyber attacks and manipulation. Part of this effort includes ensuring their physical security as well, since unauthorized physical access could enable tampering with and/or damaging of these assets.

EP#1 - Effective cyber security practices include providing adequate physical security measures to ensure that unauthorized personnel cannot gain access to critical digital assets (including their inter-connecting wiring and cables) that perform or support the functions listed in Table 4.1.

Operational environment - Adequate physical security extends beyond merely locking doors and putting padlocks on cabinets (although those are good basic physical security measures). Digital assets require clean, stable electrical power and an operating environment that is reasonably clean (of dust, airborne particulates, and corrosive liquids) and often require that both humidity and temperature are maintained within the manufacturer's stated operating ranges. At some point these assets may need to be provided with maintenance, or some level of administrative support (more on this topic in Section 7), and this means that there ought to be adequate lighting and sufficient physical space to allow support personnel to perform their authorized activities.

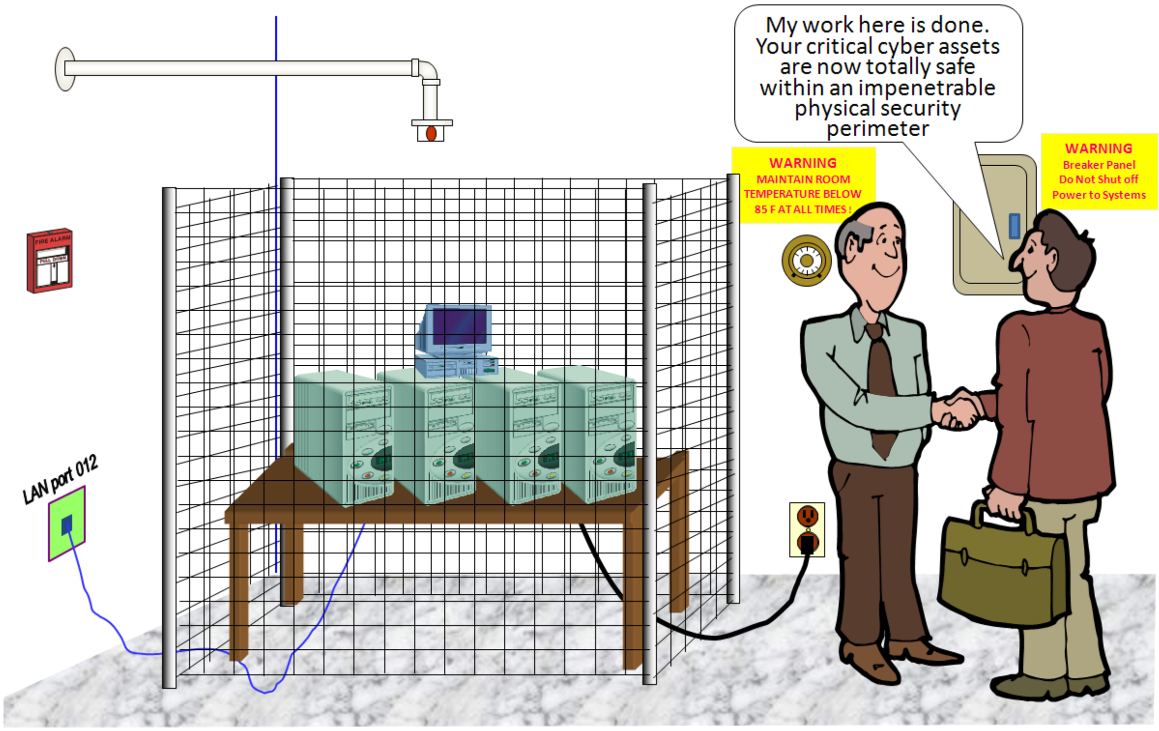

My work here is done. Your critical cyber assets are now totally safe within an impenetrable physical security perimeter
WARNING MAINTAIN ROOM TEMPERATURE BELOW 85 F AT ALL TIMES !
WARNING Breaker Panel Do Not Shut off Power to Systems
FIRE ALARM
PULL DOWN
LAN port 012

Figure 4.1 – Numerous factors need to be considered with physical security

All of this means that a range of factors must be considered when establishing the required level of physical security for CDAs. Figure 4.1 illustrates some of the common mistakes made in attempting to establish adequate physical security (and a suitable operating environment) for CDAs. Disrupting the power source to a digital asset is usually a sure-fire way to terminate its functioning. Some digital assets, based on a fail-safe design, may power-down into a safe condition. But many will just stop operating unless they have an integral battery supply or are powered from a UPS (uninterruptable power supply). And even then, it is possible that those power sources will not provide sufficient time to allow for detection and recovery. If a physical intrusion detection system (i.e., a "burglar alarm") goes onto internal battery power early on a Friday evening, will it keep operating long enough for this to be discovered when personnel return on Monday morning or after an extended holiday weekend? *.*

EP#2 - An effective cyber security practice is to provide backup power and to size the power capacity and duration (watt/amp-hours) of battery and UPS supplies to ensure that they can support continued operation for 25% longer than the worst-case time interval required for detection and response to a power outage.

Use of key locks - One of the most basic means for physically securing something is to place it into a locked room or enclosure and then control who is given a key. There are a wide range of locks today including some that use special keys and even some that don't require a key. A typical office door lockset will have a key that is fairly easy to forge or have replicated and such locks can often be picked with simple tools and a minimum amount of practice. There are lock-picking instructions readily available on the internet, including instructions on how to make lock picking tools from common household items. Figure 4.2 illustrates some lock/key variations available plus a simple key management system.

Standard industrial enclosures and cabinets with key-locks often have a standardized key system that can be defeated with minimal effort. In fact given no more information that a code number off of the enclosure it may be possible to order a replacement key. Enclosures containing CDAs, if such enclosures are the primary physical protective measure, should employ hasps and separate padlocks rather than depending on the integral keylock in the door handle of the cabinet.

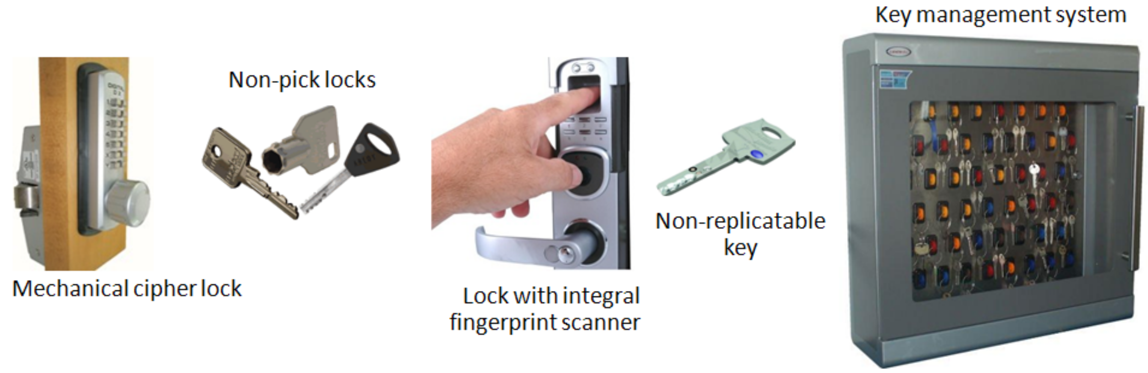


Figure 4.2 – The right type of locks and key management improve CDA security

EP#3 - An effective practice when securing CDAs using locks is to utilize non-pick door locks and padlocks that require specialized, hard-to-replicate keys. A corresponding effective practice is to employ a key management system so that keys are issued only when needed and their return is tracked.

Use of RFID ID badges- Most NPR licensees have implemented Radio Frequency Identification (RFID) personnel ID badges as part of their access control systems. RFID badges allow proximity readers at entry and egress points to support personnel identification and enable (or block) unattended entry into the licensee facilities and into critical internal areas. RFID badges use a passive token technology wherein an RFID reader activates the badge’s circuitry, and reads the contents, when the badge is brought into reasonably close proximity (see Figure 4.3 below.) Unfortunately threat actors have discovered that a simple, portable RFID reader can be built out of readily-available components. If someone with such a device is able to brush-by a person with an RFID badge, the badge contents can be read and then played-back using the same device, which is essentially like actually having the badge. This ploy is called “badge cloning.”

EP#4 – An effective practice to protect against stolen or cloned RFID badges from being is to implement a multi-factor authentication scheme to augment the RFID badge. In such a scheme some additional user-specific factor, such as a unique pass-code or PIN (something you know), or the use of biometrics (something you are), can decrease the likelihood of a stolen or cloned badge being successfully used to gain unauthorized NPR facility access.

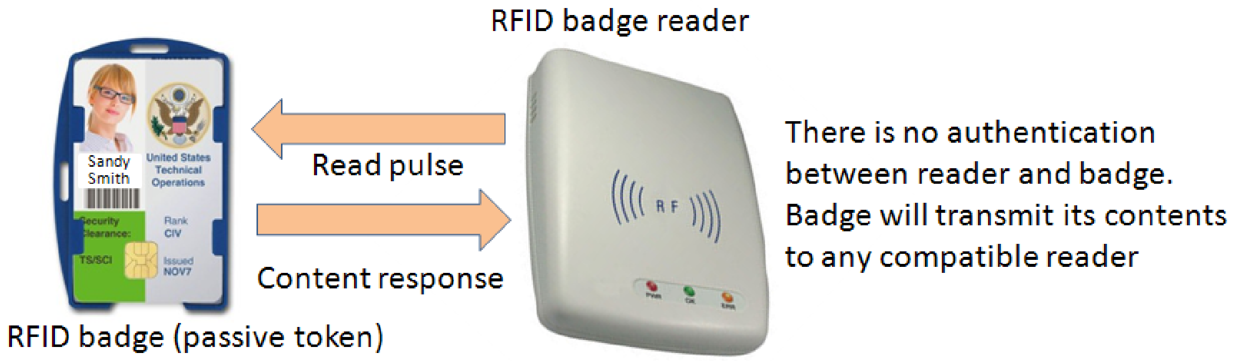

RFID badge reader
Sandy Smith
United States Technical Operations
Security Clearance:
TS/SCI
Rank CIV
Issued NOV7
Read pulse
Content response
RF
There is no authentication between reader and badge. Badge will transmit its contents to any compatible reader
RFID badge (passive token)

Figure 4.3 – RFID badge (passive token device) and compatible badge reader

RFID badge cloning can be easily defeated since it relies upon an electromagnetic connection between the badge and reader.

EP#5 - An effective practice for preventing badge cloning is to require the use of special badge carriers or covers that provide an electromagnetic shield such as ones fabricated from metalized plastic or actual metal.

Cyber attack pathways- Cyber attacks on a CDA require a series of elements/factors to be successful. First, there must be an identified vulnerability in the target CDA. Second, there must be an exploit developed to specifically take advantage of the vulnerability. Third, there needs to be a means for delivering the exploit to the target. And finally there needs to be a CDA-specific payload (software) that is inserted into the target (usually overwriting existing software) by means of the exploit and which results in altering the device/system's function(s).

Delivery of an exploit can be accomplished via any number of pathways, although the exploit used must be specifically designed for the chosen pathway. The usual pathways considered when addressing cyber security include the following:

1. Physical access to the system/device HMI (e.g., keyboard, display, panel)
2. Use of portable media with the system/device (e.g., CD/DVD, USB, SD)
3. Network access to the system/device (e.g., Ethernet LAN, WAN)
4. Serial communications to the system/device (e.g., telephone line/modem)
5. Wireless communications to the system/device (e.g., WiFi, Bluetooth)
6. Temporary connection of portable digital devices (e.g., laptop PC, test equipment) to the system/device

Table 4.2 – Pathways that can be used in executing cyber attacks

> *EP#6 - An effective cyber security practice is to eliminate or at least minimize and protect the available attack pathways that might be used by an adversary.*

There is one other pathway that needs to be considered as well. It is usually referred to as the supply chain. This issue is discussed in Section 11. For the rest of the pathways listed in Table 4.2, the discussion of associated effective cyber security practices can be found in the following sections of this document:

Physical access	item 1	Sections 4 and 5
Portable media and devices	item 2	Section 9
Network access	item 3	Section 6
Serial communications	item 4	Section 6
Wireless communications	item 5	Sections 6 and 10
Temporary connections	item 6	Section 7

> *EP#7 - An effective cyber security practice is to eliminate (or disable) unnecessary pathways to critical digital assets and then to place appropriate and adequate security controls on those pathways that remain, to protect and defend them.*

Those controls may be technical in nature (e.g., a firewall, account passwords, anti-virus software) or physical in nature (e.g., locked cabinets and/or rooms) or purely administrative (e.g., policies, procedures, guidelines, training.) An appropriate combination of the various types of controls can prevent available pathways from being used for a cyber attack.

If a digital asset has no functioning communication pathways (items 3, 4 and 5 in Table 4.2) then a cyber attack would require physical access to the asset (which could then provide access to device/system peripherals and interfaces.) This is why adequate physical protection of CDAs is essential.

EP#8 - An effective cyber security practice where a communication interface or peripheral is present, cannot be disabled, but is not (and would not normally be) used, is to physically block/lock the interface with some form of physical barrier device such as a port-lock.

Inexpensive port locks are available for USB, Modem/RJ-45 (Ethernet) and DB-9/25 (serial/"COM:") ports as illustrated in Figure 4.4. These devices can physically block access to unused ports on digital assets when such ports cannot be disabled through configuration settings or by other means.

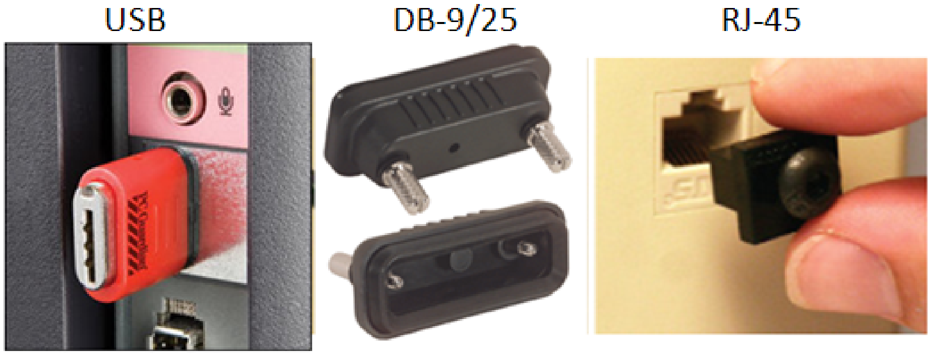


Figure 4.4 – Physical barrier (port-lock) devices used to block port access

Where a CDA has the occasional need for maintenance and administrative activities that require access to such a port, a port lock provides a means for allowing the port to remain active, while not being accessible for unauthorized use by malicious personnel.

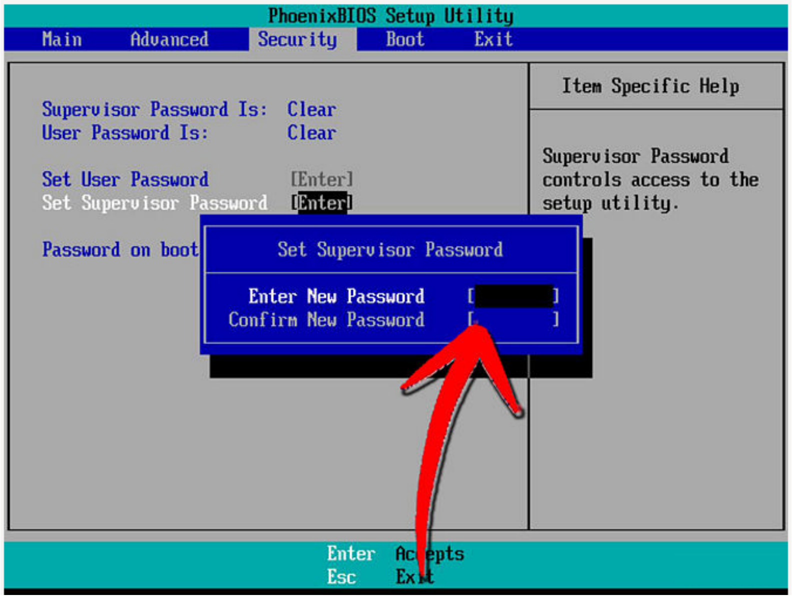
Protecting SGI- Where licensees have SGI information (including nuclear material inventory and location information) in an electronic form there are steps that can be taken to protect that information against unintended disclosure.

> *EP#9 – An effective cyber security practice for securing sensitive and classified information in electronic form is to ensure that the system, containing the information is isolated (meaning never attached to any LAN or WAN or serial communication channel) and to use either full disk encryption or folder encryption as well as setting a BIOS password to prevent unauthorized access to the system/device and disclosure of that information.*

These are capabilities (encryption and BIOS passwords) built into all modern PCs and laptop PCs today and they merely have to be enabled (refer to Figure 4.5). And of course, as with any use of passwords and encryption, the passwords and keys must themselves be kept secure and confidential. Many licensees have elected to use a dedicated laptop PC for storing electronic format SGI and then using physical measures (an approved locking cabinet or safe) to control access to that laptop PC.

> *EP#10 – An effective cyber security practice is to use a BIOS (a.k.a User) password to prevent a laptop from booting up unless one knows that password (and to use a supervisor password that will prevent unauthorized use of the setup utility itself.)*

Since an adversary with physical access to a password-protected laptop could remove the hard drive and attach it to another computer, enabling full disk or folder encryption is also a very important and highly recommended and an effective cyber security measure for protecting SGI and other information.



```
Supervisor Password Is:  Clear
User Password Is:        Clear

Set User Password        [Enter]
Set Supervisor Password  [Enter]

Password on boot
```

Set Supervisor Password

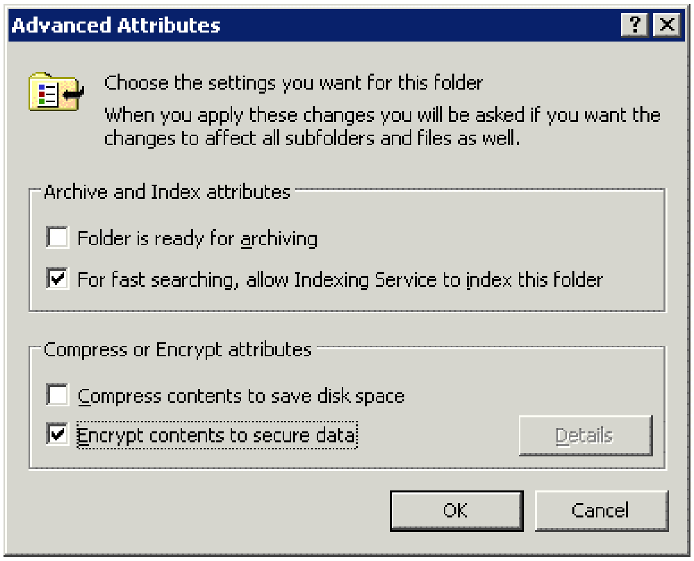
```
Enter New Password    [        ]
Confirm New Password  [        ]
```

Supervisor Password controls access to the setup utility.

```
Enter  Accepts
Esc    Exit
```

Figure 4.5 – Enabling the BIOS/User & Setup passwords on a typical laptop PC

Encryption can be done to the entire hard drive of a laptop PC using 3rd-party commercial products or Microsoft Bitlocker, but folder encryption (encryption of all files in a directory and its sub-directories) can be done with built-in EFS (encrypted file system) functionality available in most modern operating systems (such as Microsoft Windows, Linux variations, etc.) Figure 4.6 shows the file/folder attribute pane in Windows and the optional check-box to enable encryption. Such encryption is user(s)-specific such that only specifically enumerated users will be able to access the encrypted files. All others will be informed that access is blocked (even if the hard drive were removed and attached to another PC.)



Advanced Attributes

Choose the settings you want for this folder

When you apply these changes you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

□ Folder is ready for archiving

☑ For fast searching, allow Indexing Service to index this folder

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

Figure 4.6 – File/folder advanced attribute settings pane in Microsoft Windows

Setting up encryption requires more than merely checking the box; you do have to generate digital certificates with keys and list the users who will be permitted file access. But these are administrative functions that should be easily managed and accomplished by IT personnel.

EP#11 – An effective cyber security practice is to enable either full-disk encryption or selected folder encryption of computers and laptop PCs that contain SGI, classified or sensitive information.

Physical security systems- Most of the systems that provide physical security at licensee facilities are composed of multiple components physically deployed around the facility and interconnected by either a LAN or multiple serial communication circuits (or a combination of both) depending on age and technology level. Figure 4.7 shows a block diagram of a physical intrusion detection ("burglar-alarm") system integrated with an access control system and Radiation Monitoring System (RMS) units. More modern physical security systems may support greater levels of integration (more devices sharing a common LAN and interoperating in a 'plug-and-play' manner rather than requiring cross-wired

I/O signals.) But all of the facilities visited by the staff during the survey had architectures similar to the one presented in Figure 4.7.

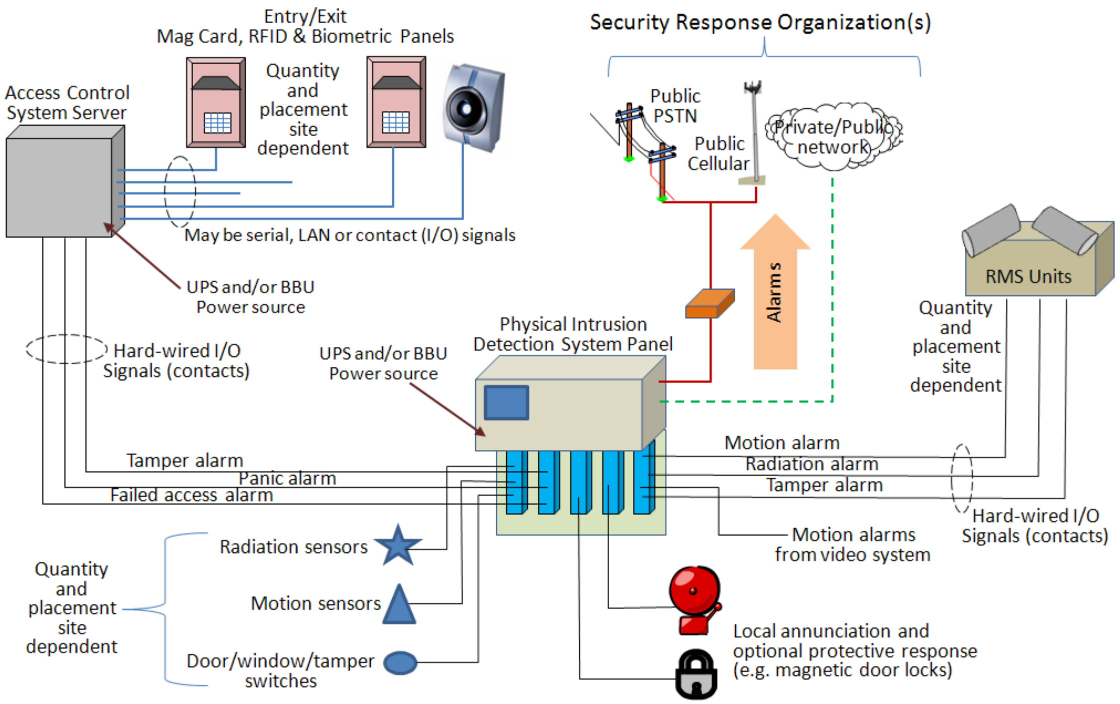

Entry/Exit
Mag Card, RFID & Biometric Panels
Security Response Organization(s)
Access Control System Server
Quantity and placement site dependent
Public PSTN
Public Cellular
Private/Public network
May be serial, LAN or contact (I/O) signals
UPS and/or BBU Power source
Alarms
RMS Units
Quantity and placement site dependent
Physical Intrusion Detection System Panel
Hard-wired I/O Signals (contacts)
UPS and/or BBU Power source
Motion alarm
Radiation alarm
Tamper alarm
Tamper alarm
Panic alarm
Failed access alarm
Hard-wired I/O Signals (contacts)
Motion alarms from video system
Radiation sensors
Quantity and placement site dependent
Motion sensors
Door/window/tamper switches
Local annunciation and optional protective response (e.g. magnetic door locks)

Figure 4.7 – Simplified block diagram of typical integrated (interconnected) access monitoring, control and alarm systems at licensee facilities

In such a setup there will be components that must be physically accessible to potentially malicious individuals, such as ID card readers, surveillance cameras and biometric/iris scanners at external entry points. These devices need to be physically mounted and installed in a manner that resists tampering.

EP#12 – An effective cyber security practice would include making use of tamper-detection functionality built into all user-accessible (and especially externally mounted) devices (or adding it) and tying that detection capability into the physical intrusion detection system as alarm inputs.

Physically distributed systems also make use of, and depend upon, inter-element wiring for communications, pow distribution, and I/O signals. All such wiring offers the possibility of tampering and is therefore a cyber attack pathway. By cutting or shorting various wires it may be possible to disable sensors and locks.

EP#13 – An effective cyber security practice is to put all such wiring into metal conduit, use metal junction boxes with anti-tamper screws, route the wiring so as to be out of normal reach and to keep it internal to the facility, except where it must be routed through walls to externally-mounted devices.

Applying passwords to digital assets- Many of the critical digital systems/devices that perform or support the functions listed in Table 4.1 are sophisticated enough to support some form of user authentication mechanism. This may be a simple, universal password/code used by anyone requiring access. Or the CDA may support two such codes; one for look-only ("read only") access and the other for making changes. In some cases the CDA may be capable of having multiple, user-specific accounts, each with a unique ID and password. It may even allow those accounts to have different levels of access to CDA settings, functions and configuration (as with a PC running a Windows® operating system.) The (factory/manufacturer) default password on most computer and digital devices can be found by a simple Google™ search.

EP#14 – An effective cyber security practice is to always change the factory default passwords on all digital devices (especially CDAs) before putting them into service. In more general terms it is an effective practice to have a password policy that defines things like how complex/strong passwords need to be and how often, or under what conditions, they need to be changed (e.g. such a policy ought to address adding and removing accounts on CDAs when personnel changes occur).

Having such a policy is meaningless unless licensee personnel are familiar with it and understand the importance of adhering to the policy. Personnel training and cyber security awareness will be discussed further in Section 8. Most of the licensees have IT organizations that are responsible for their office automation systems (possibly also their site LAN) and they may already have password and user account policies that <u>may</u> be appropriate to use with the licensee's CDAs. But most IT policies are written for PCs running a commercial operating system such as OS-X©, Linux© or Windows©. Such policies normally don't address 'smart' instruments and automation devices where password support may be quite basic and limited (e.g., a four-digit numeric code that is used by [known by] everyone who needs to access the device) and there are no user accounts.

EP#15 – An effective cyber security practice is to have a separate policy to deal with those types of specialized devices. Also if CDAs are isolated, and within the physical security of the NPR facility, then access is already severely limited and passwords may not need to be as 'strong' (complex/long), or changed as frequently, as would be recommended (for example) for a network connected PC or laptop computer. A password and user account policy needs to consider and address the following issues to be comprehensive and effective:

- *Removing/changing factory-default passwords and accounts*
- *Password complexity based on CDA capabilities*
- *Restricting who is permitted to have administrative rights*
- *Temporary accounts for vendor/contractor support*
- *Alternative protective measure where there are no passwords or they are weak and provide inadequate protection*
- *Events that should trigger account removal and password changes*
- *Maintaining an inventory of CDA passwords and accounts*

A very common way to break into systems and digital devices that support password protections is to use a brute force attack where you try all sorts of passwords, including frequently used ones (such as the word "password") until the correct one is found. Some devices can be set to lock-out account access (for some period of time or until administratively reset) after some number of incorrect login attempts.

EP#16 – An effective cyber security practice, where CDAs support account locking after a modest number of failed login attempts, is to enable that functionality to defeat brute force attacks on passwords and user accounts.

Some devices place no limit on login attempts and particularly if such a device uses a simple numeric code as a password then it is likely that a dedicated attacker will eventually discover that code and gain access to the device. If such a device/system is isolated then such an attack would have to be made physically at the system/device and if video surveillance is active this unauthorized activity should be detected. If a system/device is remotely accessible via a communication channel or network connection then such an attack could go unnoticed and undetected.

EP#17 – An effective cyber security practice, where possible, is to keep CDAs isolated (no communications connectivity) so that physical access (to the facility and CDA) is required to adjust, manipulate, configure or service the CDA.

This issue will be discussed further, in regard to performing maintenance and administration in a secure manner, in Section 9. The primary reason for requiring passwords to be changed frequently is so that, if someone is attempting to “brute-force” (guess) the password, they do not have adequate time to do so before it is changed. If a device is isolated and under surveillance, then it is far less important to change passwords based on elapsed time. In that case passwords primarily need to be changed when personnel who know the password no longer have/need permission to access the device/system (e.g., they take another job or are terminated or graduate.)

Local/isolated networks- In some cases a small set of devices/systems may need to be interconnected on a local LAN to function properly. It is possible to create an “isolated LAN” (e.g., within the reactor control room or controlled access area) to address this requirement but without introducing unacceptable cyber security vulnerabilities or creating exploitable attack pathways. Isolated LANs and their specific requirements are discussed in Section 6.

Section 5: Physical security requirements and cyber security

NPR licensees already have an obligation to meet specific physical security requirements in accordance with 10 CFR 73.60 and 73.67 and most have implemented a range of physical security measures aimed at meeting these requirements. This has included installing augmented physical barriers (e.g., gates, doors, locks) to prevent unauthorized entry into the facility and into sensitive areas within the facility. Licensees are using access control systems with digital (RFI) keycards and biometric authentication (e.g., iris scanners, hand-geometry scanners) to control and track personnel access. Licensees are using video surveillance (and recording) systems for visual monitoring of exterior entry/egress points and selected interior areas to detect and record unauthorized access and suspicious activity. They are using physical intrusion monitoring and detection systems, and environmental/radiation monitoring systems to detect unauthorized and unsafe conditions. At most of the sites the various subsystems provide alarms to the intrusion detection system in the form of hard-wired contact signals as shown in Figure 4.7. Since the primary risk/threat for most NPRs is the theft of nuclear materials, it is important that the physical systems be both physically and cyber secure themselves.

Physical security support CDAs - All of the physical intrusion detection and access monitoring and control systems observed (and some of the video surveillance systems) were based on modern digital/microprocessor technology. Since these systems and devices are digital, they themselves are potentially subject to cyber attack and manipulation. Because these are COTS (commercial off-the-shelf) products, it is easy for an adversary to obtain a copy of them (as well as vendor documentation and training) to look for weaknesses and vulnerabilities. Even if the vendor uses special proprietary software or tools to configure and administer these systems, a motivated adversary can easily acquire those same tools and software. For this reason a password on a laptop PC used for running the vendor software is of limited value since that same software can be purchased by the adversary, and loaded and run on a different laptop PC. This is not to say that the practice of password protection of laptops or PCs used for CDA support should be ignored or abandoned. To the contrary, laptop PCs should always have password protections enabled and strong passwords maintained. This scenario illustrates the importance when sourcing CDAs to specify integral password capabilities, enabling those capabilities, and assigning and maintaining strong passwords.

EP#18 – An effective cyber security practice is to utilize the integral password capabilities of all CDAs that support them by assigning them the strongest possible passwords in replacement for any vendor/factory default passwords that come pre-configured in the CDA. Default passwords should NEVER be left in CDAs due to their all-to-easy discovery.

Figure 5.1 shows how each CDA capable of supporting an integral password should be assigned a unique password (a different one for each CDA). This will block access to someone with their own copy of the vendor's tools and help to keep them from gaining access to your CDAs.

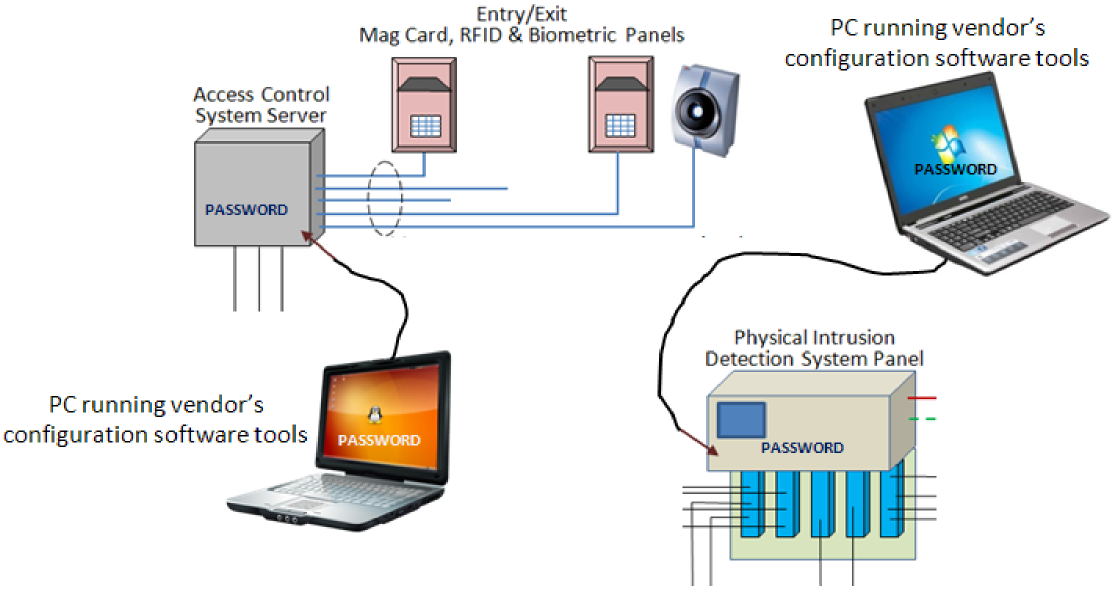

Entry/Exit
Mag Card, RFID & Biometric Panels
PC running vendor's configuration software tools
Access Control System Server
PASSWORD
PASSWORD
Physical Intrusion Detection System Panel
PC running vendor's configuration software tools
PASSWORD
PASSWORD

Figure 5.1 – Use of local/integral passwords on each CDA that supports them

Even if some of these systems, or their component elements, are not susceptible to program alteration or malware infection (e.g., because all their program code is in ROM), the malicious manipulation of selected configuration settings can often disable them just as effectively as giving them a malware virus. In general there are a set of actions and effective practices that can be applied to all CDAs, but especially those used to support physical security, and which will greatly enhance their cyber security:

EP#19 – An effective cyber security practice is to take the following actions to secure each CDA:

- *Physically protect these systems/CDAs against tampering and manipulation (place them in locked, alarmed rooms/enclosures)*
- *Implement any anti-tamper (tamper detection) alarm functions supported by the CDAs*
- *Implement unique CDA passwords to block unauthorized access*
- *Document and make a backup of valid configuration settings (hardware settings and software settings)*
- *Require administration, maintenance and configuration activities to be performed locally (no remote access)*
- *Verify/test CDA/system functionality after performing maintenance and administrative functions*
- *Logically isolate these systems or restrict them to their own isolated LAN or LAN segment (see Section 6)*
- *Physically protect the I/O, power and LAN wiring*
- *Provide adequate UPS or battery-backed power capacity*

Although always preferable, it is not always possible to require that administrative and configuration functions be performed locally. Thus, if remote support must be allowed there are steps that can be taken to make that remote access more cyber secure. Section 7 addresses remote access and administration. Just because the software tools for CDA support and configuration are commercially available from their respective vendors doesn't mean that you should not provide reasonable protections for the computers/laptop PCs you use for this purpose. Portable computers can easily become infected with malware which can be spread to your CDAs if you do not provide adequate protection. Section 9 discusses the measures that should be used to protect any computer/PC that is used for support and configuration of CDAs.

Section 6: Network architectural-interconnectivity issues

Facility network architectures - A large percentage of the NPR facilities, but not all, are associated with major universities and these NPR facilities are usually interconnected with the university wide area network (WAN). NPR facility personnel gain access to the Internet, via that university network interconnection, presumably through some form of enterprise firewall (maintained by the university IT department) placed between the university WAN and the actual Internet. This NPR facility interconnection presumably extends only to the office-automation systems used by facility personnel and not to any systems or computers associated with the operation or protection of the reactor (this was the case in each site surveyed). For NPR facilities that are not associated with a university, there is still generally some need for these facilities to be interconnected to a corporate or government WAN that serves the same function as the university WAN and, as with the university WAN, provides the NPR facilities with equivalent Internet connectivity. Figure 6.1 shows a block diagram of the typical university network structure and NPR facility connectivity.

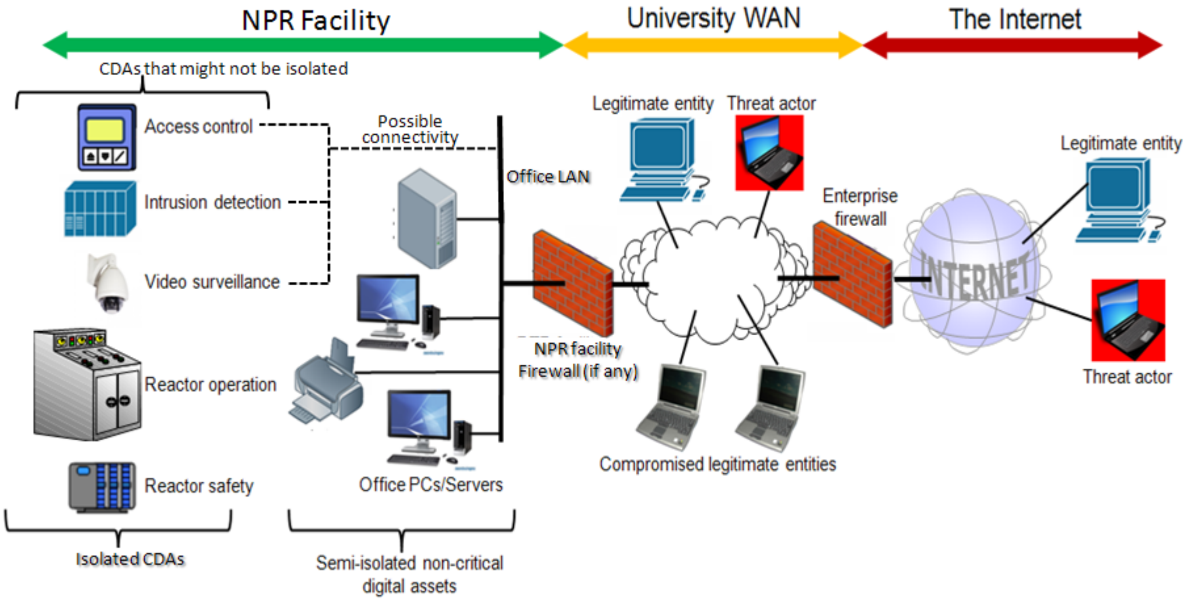


Figure 6.1 – General block diagram of a typical NPR facility network architecture

Section 6: Network architectural-interconnectivity issues

University networks (and to a lesser degree corporate and government networks) are well known to be dangerous places, from a cyber security viewpoint, because they are made available to the student body and there is limited control over what is being connected, the websites being visited by the students and the software being run on end-devices. There is often a great deal of malware being exchanged and (re)introduced around the university network because of student activities. Often the university will place firewalls in front of essential servers to restrict and control access to, and abuse of, those servers. Corporate and government networks are normally far better managed and controlled, but they are constantly under attack (from across the Internet) by a wide range of domestic and international threat actors seeking intellectual property, trade secrets and classified information. Thus the associated university/corporate/government network cannot be considered as fully trusted; and of course the Internet itself is totally untrustworthy. This means that the office automation systems and local area network (LAN) of the typical NPR facility (and any other interconnected networks and devices) are potentially subject to cyber attack from both threat actors on the Internet and threat actors on the associated university/corporate/government WAN. As long as the critical digital systems of the NPR facility are isolated (not connected to the office LAN of the NPR facility), then the worst-case scenario would be having NPR facility office PCs and servers compromised, infected with malware, and any valuable information and material they contained being destroyed, altered, and/or disclosed.

Installing a facility firewall - It was observed that some of the critical systems of licensee's facilities (refer to Section 4, Table 4.1 of this document for the criteria that identifies those systems) were based on modern digital computer technology, used COTS (commercial off-the-shelf) software and hardware, and also supported removable media peripherals such as memory sticks, CD/DVD drives, and USB ports. If such portable media is used to move software, data, files, configuration settings, or other information between office PCs and these critical systems, then malware that has gotten into the office automation systems can end up getting into the presumed-to-be isolated critical systems (there is more discussion of this specific issue in Section 9).

A firewall, or similar security appliance (see Figure 6.1), can be used to block malware delivery and attempts at the remote exploitation of the office automation systems (as well as providing notification of all such attempts). A firewall can also block communications between an adversary that has succeeded in inserting malware into internal NPR systems and that malware and prevent malware from exfiltrating sensitive information. Today it is recommended that a "next generation" firewall appliance be used since malware and attack methodologies have grown in their sophistication. These advanced capability firewalls are also called Unified Threat Management (UTM) appliances to differentiate them from first-generation firewalls.

EP#20 – An effective cyber security practice is to place some form of protective device that can inspect, detect and block malicious and unauthorized message traffic, including attempts to deliver malware, between the intermediate (university/corporate) network and the NPR facility (i.e., a UTM security appliance or 'next-generation' firewall)

Firewall rules and configuration - At some of the facilities visited by the staff, the configuration of the firewall between the NPR facility and the university WAN was poorly implemented from a cyber security viewpoint. The rule-set that allows/blocks incoming (entry) and out-going (egress) message traffic often permitted a wide range of message types not actually being used "just in case" they might ever be used and often allowed a huge range of internal and external IP addresses to be accepted as legitimate again, "just in case." In some instances there were no egress rules at all, meaning that any/all out-going message traffic was permitted. Poorly considered and implemented firewall rules can make a firewall nearly ineffective and much easier for an adversary to circumvent/defeat.

EP#21 – An effective cyber security practice for firewalls is to identify the specific message types (and port numbers) and sources/destinations (IP addresses) that are actually being used (needed) and then set individual firewall entry and egress rules for each such case and block everything else going in either direction.

Where a firewall is used to detect and block malware and cyber attacks, there is a need to regularly update the firewall with the latest “signatures” as new threats are identified. This is part of the administrative/maintenance process that is discussed in Section 7.

EP#22 – An effective cyber security practice is to ensure that firewall and malware/attack detection rules and signatures are updated on a monthly basis or any time the vendor provides notification that an essential security update is available.

In addition to having a facility firewall between the NPR LAN and the university WAN, a complementary effective practice is to install and run some form of personal PC (a.k.a. “host-based”) firewall software on each of the office automation computers and servers at the NPR facility.

EP#23 – An effective cyber security practice is to utilize personal PC firewalls (host-based firewall software) on all office automation systems, PCs and laptops of the NPR facility to augment the cyber security protection afforded by the facility firewall.

This provides a defense against malware that may accidentally be introduced via the use of portable media and portable devices, rather than coming across the network connection to the university WAN and Internet. This issue (the use of portable media and digital devices) is discussed in greater detail in Section 9. For CDAs that are capable of supporting it, a more effective approach is to install some form of host-based intrusion detection or prevention software (HIDS/HIPS). However, based on the sites surveyed, only a small number of the existing CDAs would be capable of supporting such software. This is more applicable to (and available for) computers running a Windows or Linux/UNIX operating system and may be more applicable in the future when/if licensees upgrade their reactor safety and control systems and physical security systems.

Avoiding creating inadvertent attack pathways - If the NPR facilities upgrade to modern digital instrumentation and control (DI&C), data acquisition, and automation technologies in the future there may be a need to have other LANs (other than office automation) physically distributed around the NPR facility to connect the various devices and pieces of equipment. This makes it all too possible for unintentional interconnectivity to exist between the office automation LAN and these other LANs containing assets performing safety and/or security functions. An office PC with dual Ethernet network interface cards (NICs), one for each LAN, might not be recognized by NPR personnel as creating a bridge between the two LANs.

EP#24 – An effective cyber security practice is to avoid the use of dual NICs and the simultaneous connection of any computer or “digital” device to both trusted and non-trusted networks.

This is not the same as having redundant trusted networks and having dual Ethernet NICs for redundancy purposes. That is acceptable and may be necessary to provide necessary reliability and availability. Figure 6.2 shows a simplistic conceptual example of how dual network interfaces, combined with Transmission Control Protocol/Internet Protocol (TCP/IP) networking, produces a potentially exploitable bridge. The function of the IP layer within the TCP/IP “stack” is to pass onwards messages that arrive and that are not for the computer that received the message. IP would attempt to use other network connections to try and route that message traffic. That is true for any form of IP connection, including wireless connections and even dial-up telephone connections.

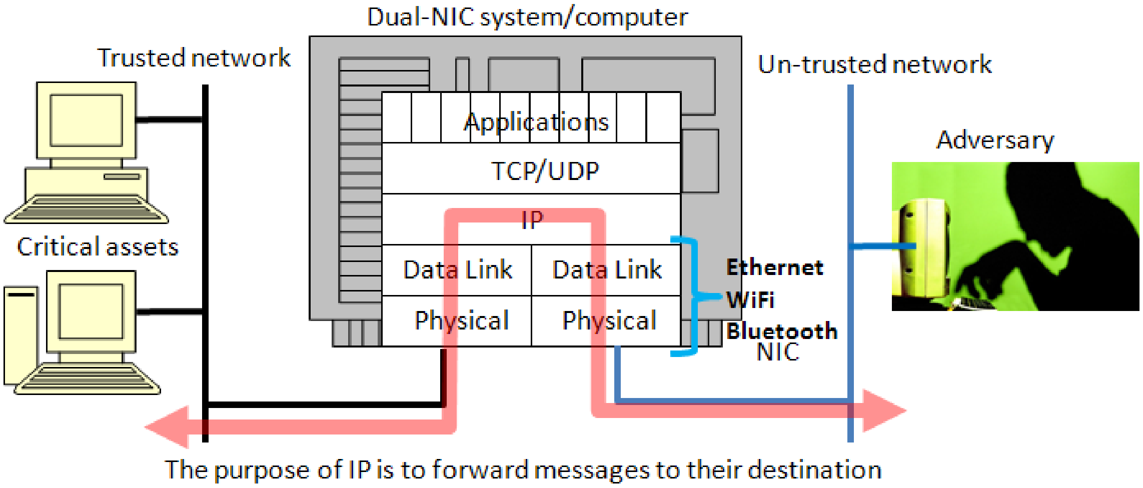


Figure 6.2 – Dual NICs creating an inter-network bridge

Note that laptop PCs today often come with both an Ethernet NIC and either/both a WiFi and/or Bluetooth NIC. Many laptop PCs still have integral telephone modems.

EP#25 – An effective cyber security practice is to always disable ALL of the wireless interfaces of a laptop PC when connecting it to a wired LAN that contains critical digital assets, or if the laptop PC is itself a CDA.

Network/LAN segmentation – Keeping CDAs isolated or constrained to an isolated LAN is always preferable. But if that is not possible and the LAN at a licensee's facility is reasonably extensive, and used to interconnect a variety of business and office-automation systems, then it becomes important to segment the LAN to provide additional protections to some of those systems. If, in the future, the LAN is expanded to incorporate systems associated with physical security and/or reactor operations, then such segmentation (along with a facility firewall) is essential. Segmentation is achieved by using transparent firewalls to further restrict the permitted flow of message traffic and to create "defense in depth," whereby an adversary has to overcome the greatest number of barriers to reach the most critical assets.

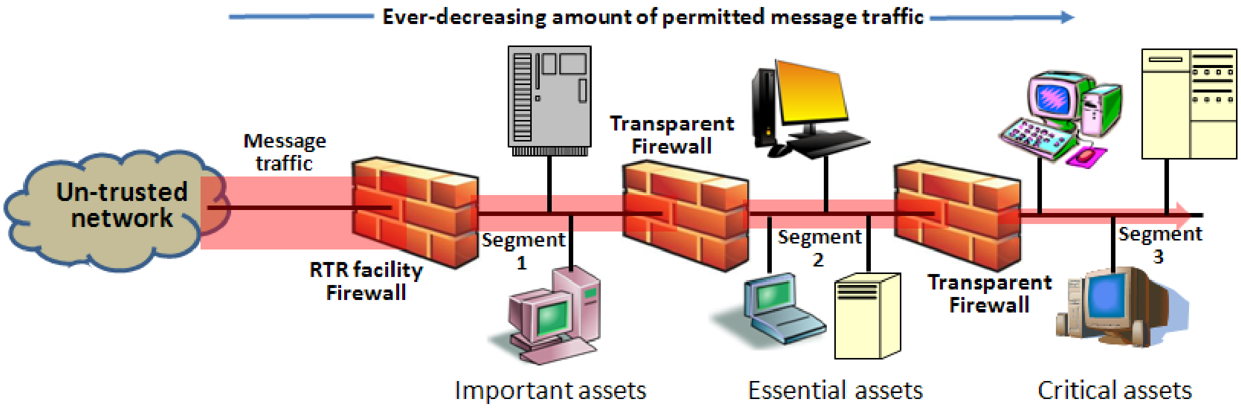


Figure 6.3 – Creating defense-in-depth with LAN segmentation

The primary NPR facility firewall will need to allow a wide range of message traffic through, much of it administrative and clerical and not related to site security or reactor functions. This being the case, additional internal firewalls can be used to further restrict message traffic to those systems/CDAs. Figure 6.3 shows the concept of creating LAN segments with greater and greater isolation (restrictions on allowed message traffic). If a facility has external network connectivity and has digital systems and assets of differing levels of sensitivity and importance connected to a common LAN, then it is important to place more sensitive assets behind more protective levels (a concept called creating defense-in-depth).

EP#26 – Although isolation is always preferable an effective cyber practice where that is not possible is to create LAN segments using firewalls, to group assets of similar importance/sensitivity into common segments, and then to place the most essential assets behind the greatest number of firewalls and the greatest number of message/traffic restrictions.

A proliferation of LANs at a facility may also result in having multiple computers that need to be accessed by the same person. A frequent means of reducing required desk space in such cases is to employ a KVM (keyboard-video-mouse) switch so that a single set of peripherals can be easily switched back and forth among the various computers. Modern USB-based KVM switches may also allow for the switching of bulk storage devices (e.g., "thumb drives") between computers (see Figure 6.4). Such switches can provide a means for malware to transfer from one connected computer to all others on the common KVM.

EP#27 – An effective cyber security practice is to avoid using KVM switches to interface with computers both on trusted and also on untrusted networks. Using them to connect with multiple computers that are all on the same trusted network is acceptable.

When a shared USB thumb drive, or other USB-connected peripheral, is switched via a KVM switch, it is equivalent to detaching the drive/peripheral from the previous computer and inserting it into a USB port on the current computer.

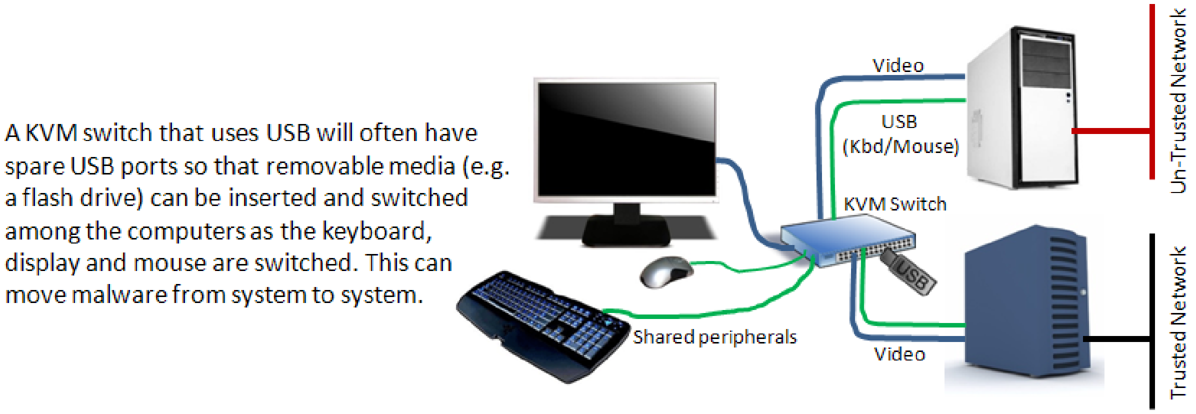

A KVM switch that uses USB will often have spare USB ports so that removable media (e.g. a flash drive) can be inserted and switched among the computers as the keyboard, display and mouse are switched. This can move malware from system to system.
Video
USB (Kbd/Mouse)
KVM Switch
USB
Shared peripherals
Video
Un-Trusted Network
Trusted Network

Figure 6.4 – Creating an attack pathway via KVM media sharing

Also a CDA could accidentally be connected to the wrong LAN (and exposed to attack) when multiple LANs co-exist in the licensee's facility.

EP#28 – An effective practice for helping to prevent accidental connection of critical systems and devices to the wrong network is to use a color-code scheme with Ethernet cables and network distribution wall plates.

In such a scheme, a specific color of cable and connector is assigned to a particular service and that color coding scheme is used from source to end-point to ensure that there is little chance of accidental misconnection to the wrong network. Figure 6.5 shows examples of the colors available for both Ethernet (CAT-5/CAT-6) cables and wall-plate connectors. And of course all LAN wall plates should have labels that clearly identify the category/usage of each network connection.

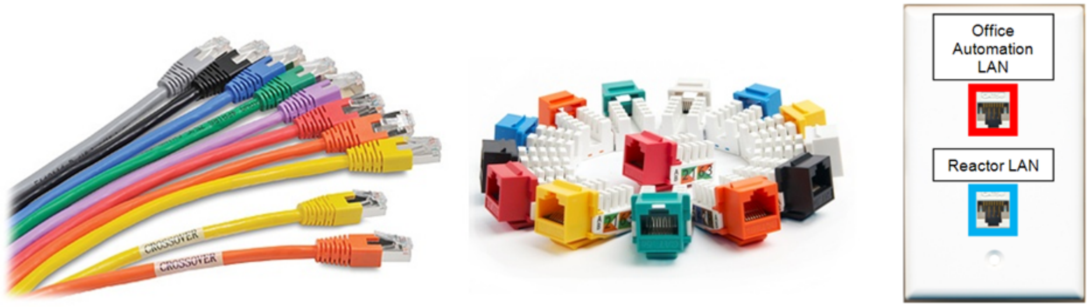


Figure 6.5 – Examples of the color variations available for Ethernet LANs

If reactor safety and control functions eventually migrate onto digital platforms and rely upon the availability of a digital LAN to function, then it is important that such LANs be made adequately reliable as well as being kept isolated from other networks.

EP#29 – An effective means for achieving LAN reliability is to implement separate, totally replicated LANs with independent media (cables) and active elements (e.g., switches). Based on the capabilities of the various devices some may support dual LAN connections while others may need to be manually or automatically switched from failed LAN to operational LAN when/if necessary.

Industrial serial communications - A large number of “smart” instrumentation and automation devices now support some form of Ethernet-TCP/IP network connectivity. Many of these devices had (and may still have) communication connectivity support for some form of non-Ethernet industrial instrumentation bus (a so-called “fieldbus”). This functionality and its associated cyber security implications will be discussed further in Section 10. But, many smart devices also support serial communications using point-to-point (or multi-point) low-speed, communication connections and some form of simplistic “industrial” protocol such as Modbus RTU or DNP3.0. Such communication connections are generally used to retrieve process measurement and status information, although they may also be used to control the process outputs of the smart device (if it has any) and to set operational parameters into the smart device (if the device is performing any local control functions and/or calculations). Such serial connections may be based on an EIA/TIA-232, 422, or 485 electrical circuit and operate either synchronously or asynchronously at data rates between 1200 b/sec (bits per second) and 128 kb/sec. Figure 6.6 shows a basic example of such a communication scheme.

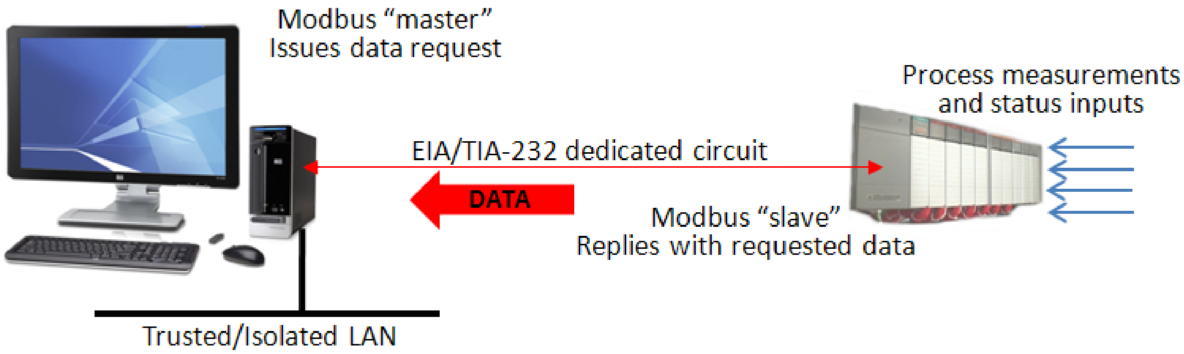


Figure 6.6 – Dedicated, low-speed, serial communications circuit using Modbus

Such communications schemes normally do not provide a cyber attack pathway onto the trusted/isolated LAN to which the critical safety/security or reactor operational equipment (critical digital asset) may be attached. The worst-case scenario (for a device with only process inputs) would be if an attacker were to hijack (connect onto) the communication circuit and send false data to the requesting computer/CDA. This would require physical access to the circuit or smart device. Even in the case where a smart device may have process outputs that are used to control reactor or facility equipment (e.g., an analog signal used to position a control rod or a contact output used to start/stop a cooling pump), any cyber attack would still require physical access to the communication circuit or the smart device and so physical protection of the circuit wiring and smart device (combined with existing physical security measures such as access control) would again be effective as a cyber-security deterrent.

EP#30 – An effective cyber security practice for 'serial' industrial protocol interfaces to digital ("smart") devices would be to protect the circuit wiring and smart device with physical barriers such as using metal conduit and junction boxes for the circuit wiring and using locked, alarmed (door switches wired into the physical intrusion detection system) enclosures for the smart devices themselves.

These legacy industrial protocols were designed to operate over noisy, intermittent, and faulty communication channels and they are implemented as highly-detailed state machines and thus the communication driver software usually incorporates a great deal of message validation and error checking that would block any attempt to exploit and attack the “master” computer or “slave” device (in an arrangement such as indicated in Figure 6.6) with specially crafted malicious messages or a buffer overflow attack.

Note – it is possible to tunnel (encapsulate) asynchronous, serial communications within Ethernet-TCP/IP packets such that this traffic can pass through LANs and WANs to avoid the need to run separate cabling. Devices called terminal servers and remote port servers can be attached to an Ethernet network to accomplish this tunneling function. Although this is a wiring convenience, it opens up the message traffic to a much greater range of potential cyber tampering and manipulation.

EP#31 – An effective cyber security practice for ‘serial’ industrial protocol interfaces to digital (“smart”) devices is to use dedicated wiring for such communications (and to use media conversion to increase distance and noise immunity if needed) and avoid ‘tunneling’ such communications through Ethernet-TCP/IP networks.

Protecting essential communications - NPR licensees are expected to maintain adequate physical security for their facilities and to have procedures for responding to physical security events and incidents. Part of this involves coordination and communication with local responders, possibly local law enforcement or campus security organizations. In some instances the NPR licensees are also using the network connectivity between the NPR facility and the university WAN (and possibly from there onto the Internet) as a means for dispatching site alarms to security responders (campus or local police) and in some instances also offering those responders remote access to on-site surveillance video streams. Some sites contract with third-party monitoring services, especially outside of normal working hours, to monitor for alarms/events from the intrusion detection system and to contact NPR personnel and designated law enforcement/security organizations when needed. Thus it is important that such essential cross-network communications be reliable, secure, and trustworthy.

Securing communications with VPNs - Message traffic traversing an untrusted public network (such as the university WAN and the Internet) can potentially be blocked or altered or spoofed (faked.) In the case of video, it may also be accessed by the threat actor and used to plan/support a physical attack. It is nearly impossible to prevent interference with message traffic traversing an insecure network, but in the case of alarms licensees have multiple, diverse means for ensuring alarm delivery (e.g., network plus analog phone and/or cell phone). Cyber tampering with a video stream traversing a network can include blocking that video stream, eavesdropping on the stream, or injecting false video into the stream. Blocking the video stream so that it no longer reaches the intended destination may actually initiate a security response, eliminating it as a viable attack method. The main cyber security issues with streaming video traversing an insecure network is preventing the adversary from accessing or viewing the security video and ensuring that responders can detect attempts to send altered or spoofed video. Figure 6.7 shows a simple means for achieving this result using VPN (virtual private network) technology.

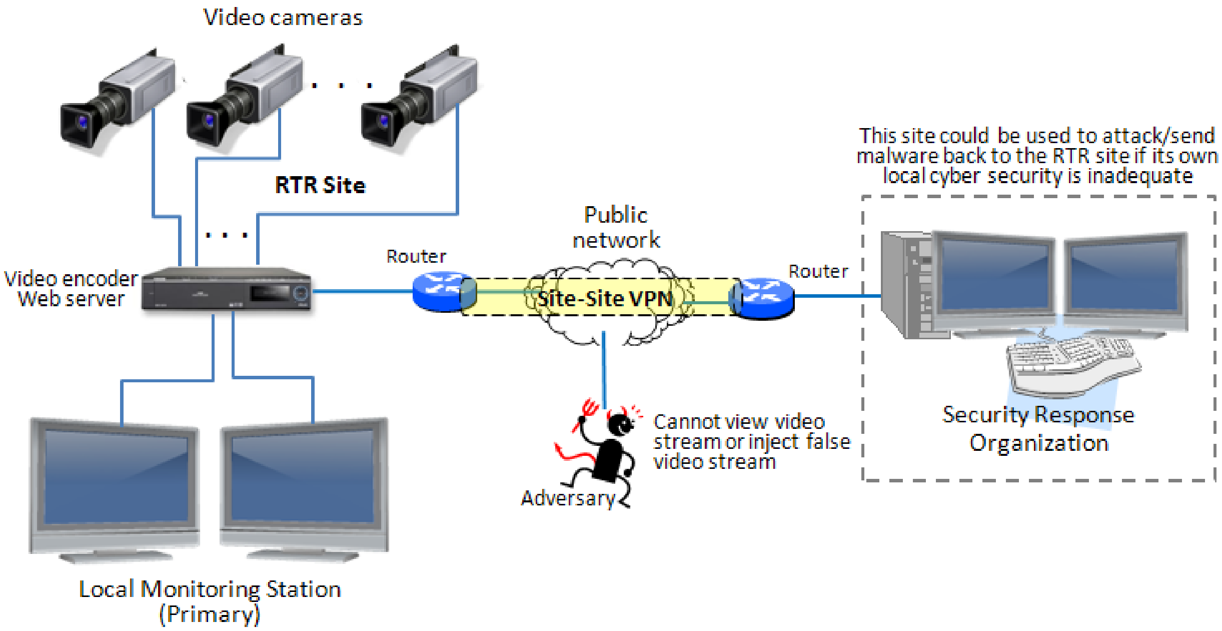

Video cameras
RTR Site
Video encoder
Web server
Router
Public network
Site-Site VPN
Router
This site could be used to attack/send malware back to the RTR site if its own local cyber security is inadequate
Security Response Organization
Cannot view video stream or inject false video stream
Adversary
Local Monitoring Station (Primary)

Figure 6.7 – Creating a site-to-site VPN using routers to encrypt video stream

In simple terms, a VPN is the application of cryptographic tools to allow the sender and receiver of messages to verify/authenticate each other (and to detect falsified attempts to send spoofed message traffic), to identify messages that have been tampered with, and to ensure that messages are unusable if accessed by unauthorized parties. The technical details are not important in this discussion. What is important is to understand that creating a VPN is often as simple as enabling that functionality in (or adding that functionality to) network devices (e.g., routers) at the sites that need to communicate in a secure manner. A VPN-protected connection is sometimes called creating a "secure tunnel" through an insecure public network.

EP#32 – An effective cyber security practice for protecting important and sensitive network traffic (video or otherwise) from tampering, unauthorized access and spoofing would be to create a permanent site-to-site VPN by putting commercial VPN gateway devices (often just routers with special software) at both "ends" of the permanent communication channel.

In this case the two "ends" would be at the NPR facility and also at the facility of the security organization that needs access to the video stream. If routers are already in place, it may be possible to add the VPN functions to those devices. VPN gateways encrypt/decrypt all message traffic and enforce the required authentication of any computer/device attempting to establish a communication connection which both prevents unauthorized access to the video and blocks attempts to falsify a video stream. Note: with a site-to-site VPN, any malware or cyber intrusion that occurs on the systems and network at one site can spread through the VPN connection to the other site(s).

EP#33 – An effective cyber security practice is to ensure/verify that the security organization monitoring the NPR facility alarms and/or surveillance video stream itself have an effective cyber security program or else their systems (and the VPN connection to the NPR facility) could provide a cyber attack pathway back to the CDAs at the NPR facility.

Isolated LANs - In some cases a small set of devices/systems may need to be interconnected on a local LAN to function properly or perform all required functions. If the LAN cabling and active elements (e.g., switches) are all contained within an access-controlled common area and under adequate physical protections (including video surveillance), and there is no interface, bridge, or gateway that connects with any other network, then this is essentially an isolated LAN and the interconnectivity doesn't present the level of cyber security vulnerability as would having this LAN extend out to and connect with the office automation LAN or campus LAN.

Section 6: Network architectural-interconnectivity issues

EP#34 – If a set of CDAs, and/or CDA-associated components, cannot operate properly or effectively without a shared local area network connectivity then an effective cyber security practice is to create and maintain a dedicated, local, isolated LAN to interconnect them including providing adequate physical security for the isolated LAN components, active elements (e.g., a switch) and cabling/media.

To qualify as an isolated LAN, there can be no network components which are shared with other networks or communication connections with other networks via bridges, gateways, routers, or other such components. (It is acceptable that a common power source be used to supply an isolated LAN and other network devices.) Using the VLAN grouping functionality of a large Ethernet switch to create an “isolated” subnet (sharing a switch with other subnets) is not adequate to be considered as being an isolated LAN. Physically separate switches should be used. Figure 6.8 shows an example of a small isolated LAN containing interconnected CDAs and other devices/systems. Note that the use of “serial” industrial protocol communications between a CDA and other smart device (as was discussed earlier in this section) does not invalidate the isolated LAN concept. The use of legacy (non-Ethernet) industrial fieldbus LAN technologies (see Section 10) will generally also create an isolated LAN. Only connectivity with other LAN/WANs would negate the isolation.

EP#35 – An effective cyber security practice is to keep all network-connected CDAs associated with a given function (e.g., physical security, reactor control and protection, emergency response) on their own, individual isolated LANs (or LAN segments) to reduce their vulnerability to cyber attack and compromise.

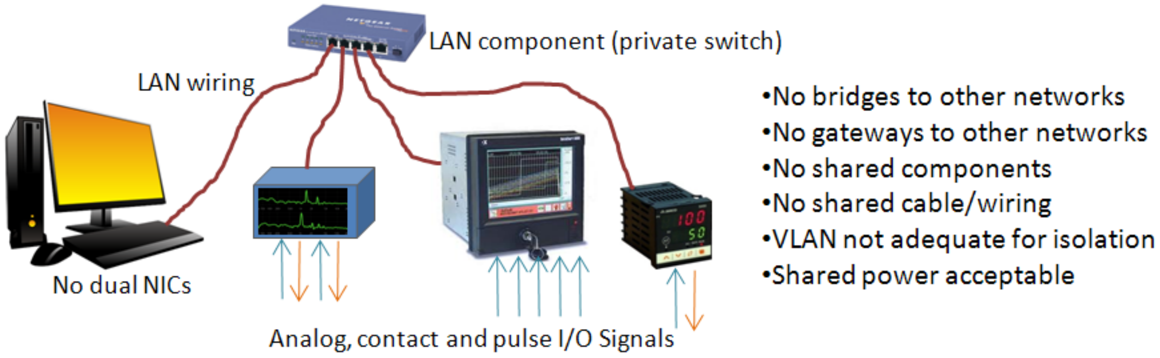

LAN component (private switch)
LAN wiring
•No bridges to other networks
•No gateways to other networks
•No shared components
•No shared cable/wiring
•VLAN not adequate for isolation
•Shared power acceptable
No dual NICs
Analog, contact and pulse I/O Signals

Figure 6.8 – Example of a small isolated LAN containing multiple CDAs

Secure use of wireless communications- Wireless networking in the form of wireless Ethernet (IEEE 802.11a,b,g, [and now ‘ac’ and ‘ad’] also known as “WiFi”) is a very convenient way to allow for flexible and ad hoc connectivity to a LAN infrastructure. Most of the licensee facilities have WiFi© routers on their office automation LAN and most universities have WiFi© routers on their campus WANs. Wireless networking, due to its radio-based nature, is subject to interference, spoofing (false/fake messages transmitted), and snooping (unintended/undesired reception of transmitted messages). There are technical solutions available within the IEEE 802 standards to address some of these issues. Conventional WiFi© uses direct-sequence spread-spectrum (DSSS) transmission which is highly resistant (but not totally immune) to interference. All forms of wireless communications are potentially susceptible to being blocked or scrambled by interference.

EP#36 – An effective cyber security practice is to avoid the use of wireless communications for essential, critical and reactor-safety functions. Hard-wired connections should always be employed for those functions and applications.

Since wireless communications can be spoofed and snooped, security mechanisms such as WEP (Wired Equivalent Privacy), WPA (WiFi Protected Access), and IEEE.802.11i have been developed to provide authentication and encryption of wireless Ethernet communications. WEP was the original cryptographic scheme deployed with IEEE 802.11a and b, but it turned out to contain many weaknesses and is now considered to be essentially ineffective at protecting wireless communications.

Today the recommendation is to employ WPA (actually version 2) which has two variations: WPA-PSK (Pre-Shared Key; also called WPA personal version) and WPA-Enterprise (also called WPA-802.1x or sometimes just WPA.) In a small office with a limited number of wireless clients, WPA-PSK may be adequate to provide effective cyber security. On a campuswide network with many wireless access points and many wireless clients, it is essential to employ WPA-Enterprise (as long as there is a centralized user authentication [“RADIUS”] server). Figure 6.9 shows the major difference between the two schemes: local versus centralized authentication and individually encrypted wireless connections between the router (access point) and each mobile client versus a single key used by all mobile clients.

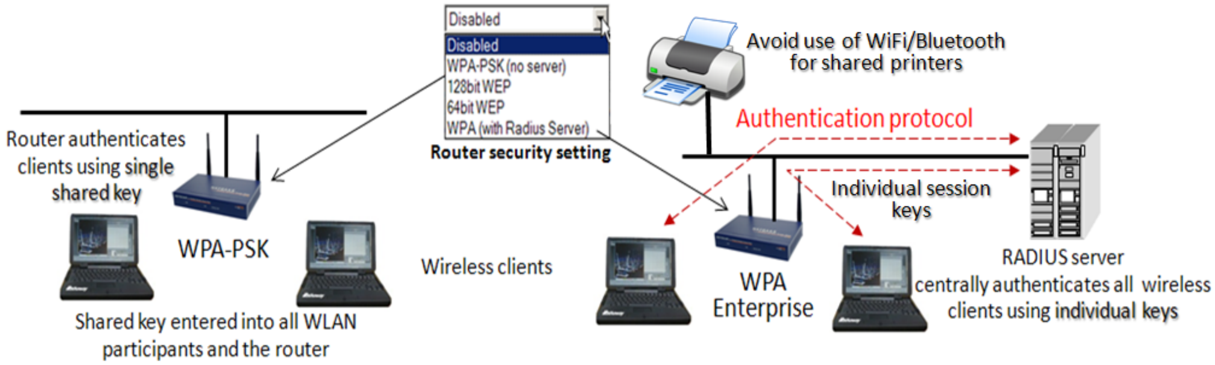

Disabled
Disabled
WPA-PSK (no server)
128bit WEP
64bit WEP
WPA (with Radius Server)
Router security setting
Avoid use of WiFi/Bluetooth for shared printers
Authentication protocol
Router authenticates clients using single shared key
WPA-PSK
Individual session keys
Wireless clients
WPA Enterprise
RADIUS server centrally authenticates all wireless clients using individual keys
Shared key entered into all WLAN participants and the router

Figure 6.9 – Using WPA-PSK and WPA-Enterprise for wireless networking

In the PSK mode one password (called a “key”) is applied to ALL wireless clients and the wireless router(s), and it must be stored on all of the wireless clients (and routers), therefore, anyone using one of those client computers can both connect to the network and also see the shared password. Since all users have access to the common password, it becomes necessary to periodically change it when users are no longer authorized, leave, change jobs, or a laptop is lost. This can be cumbersome if there are numerous wireless clients and routers involved. In WPA Enterprise mode, a wireless client authenticates through the wireless router (or AP) to a central server and then a unique (one-time) session key is generated by the server and used for the communications between only that specific client and the local wireless router. Thus every wireless client gets a new, unique key each time it connects to the network, and users never see that information. But, Enterprise mode does require staging a suitable IEEE 802.1x compatible central authentication server.

EP#37 – An effective cyber security practice for securing wireless Ethernet networks (WLANs) is to deploy and enable WPA2 cryptographic functions in all wireless routers and wireless clients using WPA-Enterprise mode and to have a central server for user authentication and to generate individual session keys for each wireless client.

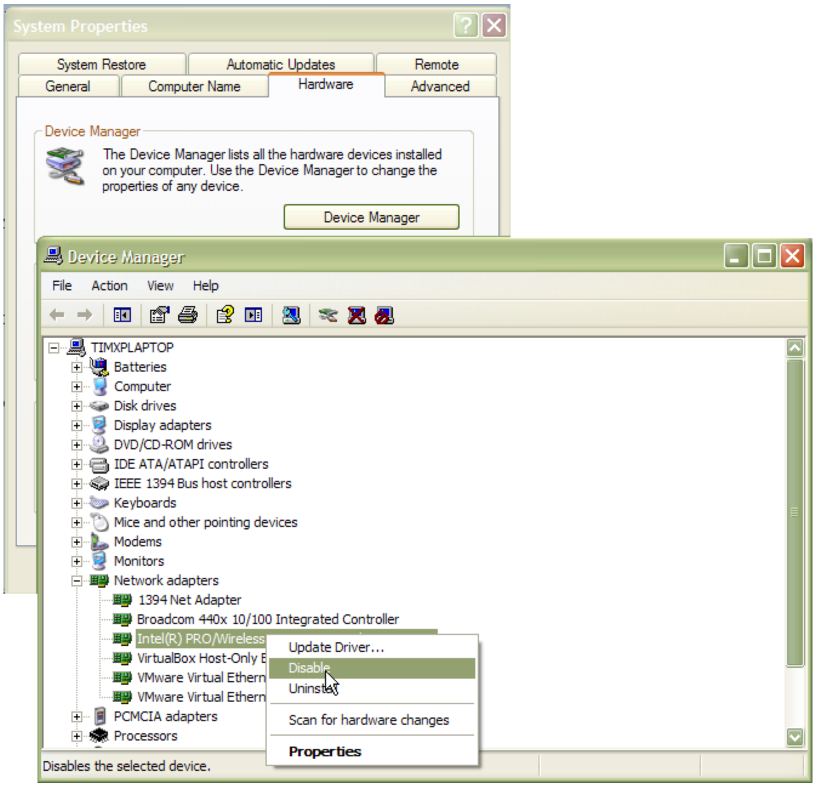
Devices like printers, copiers, and scanners that have built-in WiFi support may be capable of WPA-PSK but may not support WPA Enterprise. These kinds of devices, if compromised themselves, have been known to be used as a platform to deliver malware to other computers and devices. For that reason, it is best not to make such devices sharable via wireless Ethernet (or Bluetooth).

EP#38 – An effective cyber security practice is to disable the WiFi (and Bluetooth) capability on printers, scanners and other such network-shared peripherals and to attach those devices to a wired LAN segment (per Figure 6.9) for the purpose of making them sharable-by/available-to multiple users.

Today more and more digital devices come equipped with Bluetooth© wireless networking support. Bluetooth technology is designed for low-power, short-distance network interoperability between and among devices such as cell phones, laptop PCs, printers and many other "smart" devices. There is an ever-growing array of malware designed to be propagated via Bluetooth connectivity. Bluetooth implementation on some devices only partially supports the full security model making these devices far too easy to compromise. For that reason it is best not to make use of Bluetooth on critical systems/CDAs and to employ hard-wired connections.

EP#39 – An effective cyber security practice is to disable Bluetooth (plus WiFi and any other form of wireless) communications capability on all computers and devices connected to a trusted LAN/WLAN.

As was mentioned earlier in this section, a computer with TCP/IP networking that is connected to a wired LAN (e.g. Ethernet) and which has a wireless adapter enabled (e.g., A cellular, WiFi or Bluetooth adapter) can act as a bridge/router and provide a pathway for an attack on the CDAs connected to the wired LAN. Disabling (and later re-enabling) wireless capability is usually easily accomplished as long as you have administrative rights on the computer. Figure 6.10 shows the System Properties panel within the Windows XP operating system and the Device Manager sub-panel where individual network adapters (both wired and wireless) are listed and available to be enabled or disabled.



The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.

Disables the selected device.

Figure 6.10 – Disabling/Enabling a wireless adapter under Windows XP®

Cell phones - Some cell phones also offer a WiFi “hot spot” capability (they act as a WiFi access point and route message traffic to/from the Internet via the cellular telephone system). Having such a cell phone operating near WiFi-enabled devices could inadvertently cause those devices to automatically (without any notification) re-associate (stop communicating via the valid access point and switch over to the phone’s hot spot) opening up an attack pathway from the Internet to the device.

Section 6: Network architectural-interconnectivity issues

EP#40 – An effective cyber security practice is to require cell phones with hot-spot functionality to be turned off or kept out of any area where WiFi enabled CDAs are in use.

(And of course physical security prohibitions on allowing cell phones with cameras into sensitive areas of the NPR facility must also be observed.)

External access to reactor measurements - Since most of the NPR licensees are major universities doing research and providing educational programs in nuclear engineering, nuclear chemistry, nuclear physics, et cetera, it may be highly desirable to make reactor operating information and experimental data available, to entities outside of the NPR facility, in near-real-time. The primary cyber security issue in doing this is to prevent such communication connectivity from creating an exploitable attack pathway in reverse that allows for a compromise of the reactor safety or control functions. As has been mentioned, currently the reactor safety systems (and most of the reactor controls) are hard-wired and do not employ digital technologies. But in the future this could change and so creating a means for providing reactor data to external entities needs to be done in a manner that would not endanger the cyber security of those future systems. There are multiple approaches that can be used to provide external access to data while blocking access to the systems from which the data originates. One approach is to place a "data diode" device between the critical systems and the external entities. Another approach is to create a "demilitarized zone" (DMZ), a separate protected network segment, that contains a data server. Figure 6.11 illustrates the data diode strategy whereby a simplex (one way) communication channel is used to eliminate any possibility of message traffic flowing back in the opposite direction.

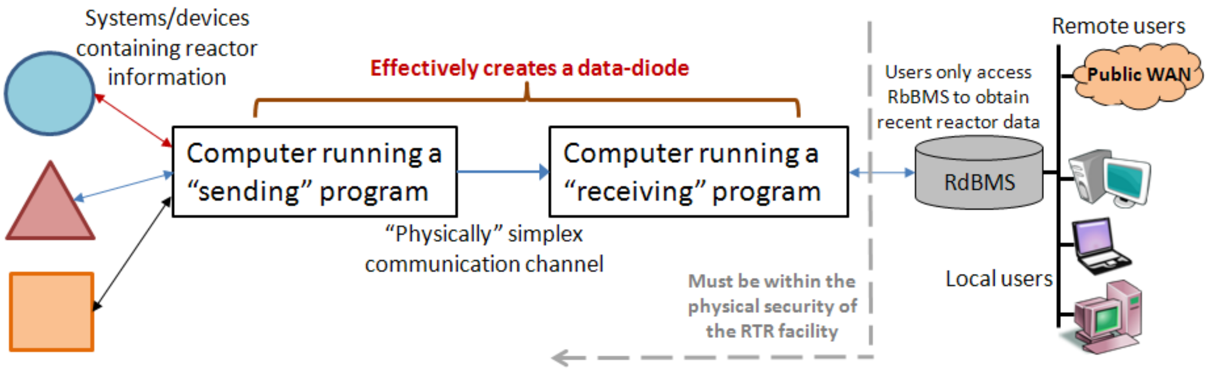

Systems/devices containing reactor information
Effectively creates a data-diode
Computer running a "sending" program
Computer running a "receiving" program
"Physically" simplex communication channel
Must be within the physical security of the RTR facility
Users only access RbBMS to obtain recent reactor data
RdBMS
Remote users
Public WAN
Local users

Figure 6.11 – Creating a one-way data flow using a data-diode

A commercial or home-brew data diode will consist of two computers connected to each other by an electrically simplex communication channel. One computer (on the left in Figure 6.11) will be programmed to collect data and transmit it to the other computer (on the right in Figure 6.11) via the simplex channel. The other computer will be programmed to receive data from the simplex channel (possibly placing it into a database server of some type) and make it available to others. Although it is possible to custom-build a data diode, there are commercial vendors of data diode products for Ethernet-TCP/IP networks.

EP#41 – An effective cyber security practice for securely transferring information from critical systems/CDAs (on trusted networks) to untrusted systems and networks is to use a 'data-diode' device to create a simplex channel that physically makes any/all reverse communications impossible.

Another commonly used means for making data available in a cyber secure manner is to create a dedicated LAN segment between a trusted and untrusted network using two routers and to place a hardened database server within that LAN segment. This approach is illustrated in Figure 6.12. The computers on the trusted network can send data update messages ("Writes") to the database server (possibly an RdBMS – relational database management system) but cannot send any messages through to the computers on the untrusted network.

Section 6: Network architectural-interconnectivity issues

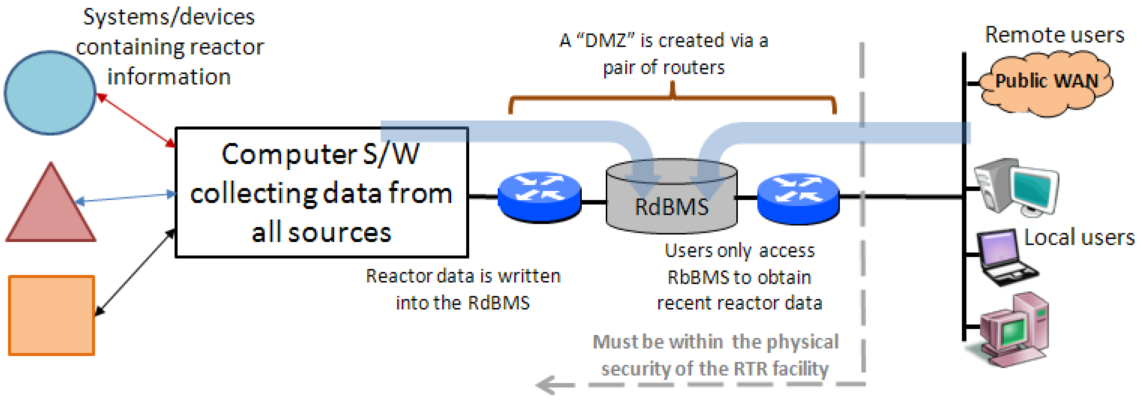

Systems/devices containing reactor information
Computer S/W collecting data from all sources
A "DMZ" is created via a pair of routers
RdBMS
Reactor data is written into the RdBMS
Users only access RbBMS to obtain recent reactor data
Must be within the physical security of the RTR facility
Remote users
Public WAN
Local users

Figure 6.12 – Creating a DMZ and shared data server to isolate networks

The computers on the untrusted network can send data access request messages ("Reads") to the RdBMS but cannot send any messages through to the computers on the trusted network. Most IT personnel will be familiar with how to configure routers to create a DMZ, a demilitarized zone (including using packet-filtering rules in each router to block all but the pre-authorized messages), and how to harden the RdBMS server to prevent it from being compromised. (Hardening is the process of minimizing the exploitable vulnerabilities of a computer system by taking actions such as patching, removing unnecessary components and services, implementing white-listing, blocking unused TCP/UDP ports, etc.) The data-diode approach is definitely more secure since it is physically impossible to send even a single data bit back across the simplex channel. With the DMZ approach an adversary on the untrusted network can communicate with and attack the RdBMS server; so if that server is not sufficiently hardened and if it is compromised it can then be used as a platform to attack systems on the trusted network. If a shared database server in a DMZ is used to make data externally available, then it is essential that it be dedicated and hardened and secured with white-listing or some other form of HIDS (host intrusion detection system) application.

EP#42 – An effective cyber security practice, where a DMZ-positioned server is used to provide reactor data to external users, is to ensure that all possible steps are taken to harden the server (including installing a white-listing application), to keep the server updated and patched, to restrict the server to only performing that specific function and to exclude any other system/device from being placed within the DMZ.

"Analog" Input/Output (I/O) data transfer – Another way for creating a semi-real-time unidirectional transfer of a small number of reactor parameters, in a manner that avoids creating an attack pathway, is to use analog (and contact) I/O signals as a means for transferring the values. This scheme has accuracy/precision limitations since the numeric data to be conveyed is converted to a voltage and then converted back again to a numeric value using 16-bit digital-to-analog (D2A) and analog-to-digital (A2D) circuitry, but that may be adequate for some applications. Of course contact outputs can be used for conveying two-state (e.g., running/off, high/normal) indications. Figure 6.13 shows an example of this approach using either simple I/O hardware or devices such as programmable logic controllers (PLCs) to handle the analog (and contact) signal generation and reception.

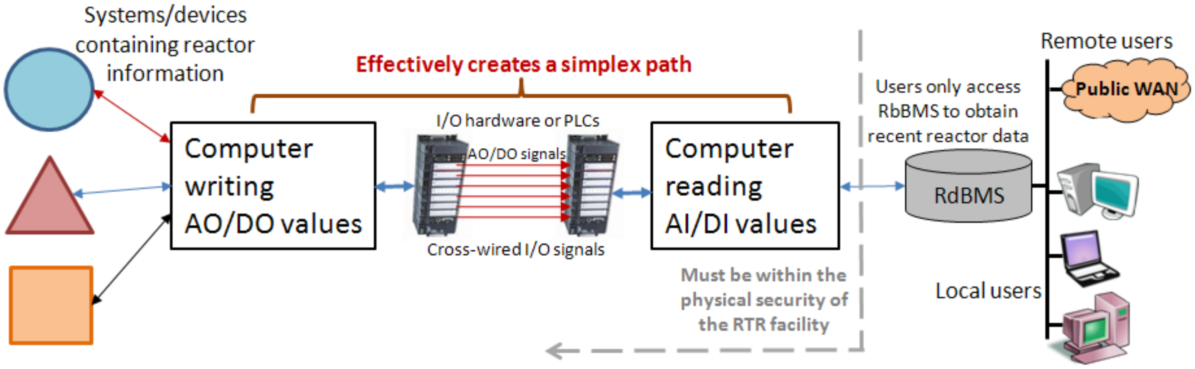

Systems/devices containing reactor information
Effectively creates a simplex path
Remote users
Public WAN
Users only access RbBMS to obtain recent reactor data
I/O hardware or PLCs
AO/DO signals
Computer writing AO/DO values
Computer reading AI/DI values
RdBMS
Cross-wired I/O signals
Must be within the physical security of the RTR facility
Local users

Figure 6.13 – Using analog and contact I/O for unidirectional data transfers

Since both A2D and D2A circuits are electrically unidirectional in nature (the transformation process is one-way), linked together they form an electrical circuit that is unidirectional. Commercial I/O modules usually support multiple signals (e.g., 4 analog outputs, 8 analog inputs, 16 contact outputs, 16 contact inputs) and so it is possible, with just a few such I/O modules, to deliver a dozen numeric values and a dozen status signals in this manner.

Additional Network Protections – The NPR facilities surveyed generally had no LANs interconnecting the equipment and devices used for reactor operation or protection, although this could change in the future. Some licensees did connect their physical intrusion detection systems and/or access control and video surveillance systems into campuswide networks. This was done to allow for centralized administration, support and remote monitoring of those systems (this is discussed further in Section 7). A network physically dispersed around a large campus, with media running between, and active components (e.g., switches) positioned within most buildings would be almost impossible to totally monitor and protect.

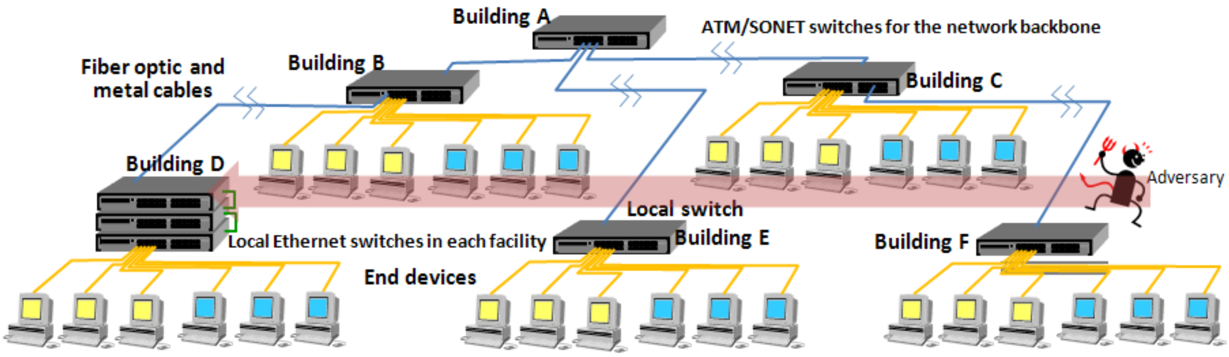

Building A
ATM/SONET switches for the network backbone
Fiber optic and metal cables
Building B
Building C
Building D
Adversary
Local switch
Local Ethernet switches in each facility
Building E
Building F
End devices

Figure 6.14 – A campus-wide network offers many points of access/attack

There are just too many places where unauthorized access would be possible by a determined adversary. With many such networks access at any point on the network provides communication connectivity to all other points on the network (see Figure 6.14) unless something prevents this from happening. Where it is not viable to keep critical NPR systems (e.g., intrusion detection, access control, reactor safety) isolated within the NPR facility, it becomes very important to be able to detect attempts to penetrate, tamper with, and compromise such systems (whether such efforts are successful or not). Local administration is always preferable but if that is not possible, then it is important to be aware that any firewall placed between the NPR facility LAN and the campus network that is configured to allow message traffic through for remote system monitoring, maintenance, and/or administration contains potentially exploitable security holes (see Figure 6.15) in addition to the well-known security holes that enable web browsing and email from within the NPR facility.

EP#43 – Where remote (cross-network) access is allowed for administrative and/or maintenance support of CDAs, because of the need to allow for firewall rules to pass such traffic, an effective cyber security practice would be to install a network intrusion detection system (NIDS) on the NPR facility LAN to inspect all message traffic entering and exiting to identify malicious, suspicious, unauthorized and questionable messages and provide a notification to appropriate NPR administrative personnel.

By "holes" we mean firewall rules that specifically identify and pass message traffic that appears to be any of the permitted types, such as web browsing and email, and which once identified by an adversary may be exploited by crafting malicious message traffic that has the same appearance as the permitted message traffic.

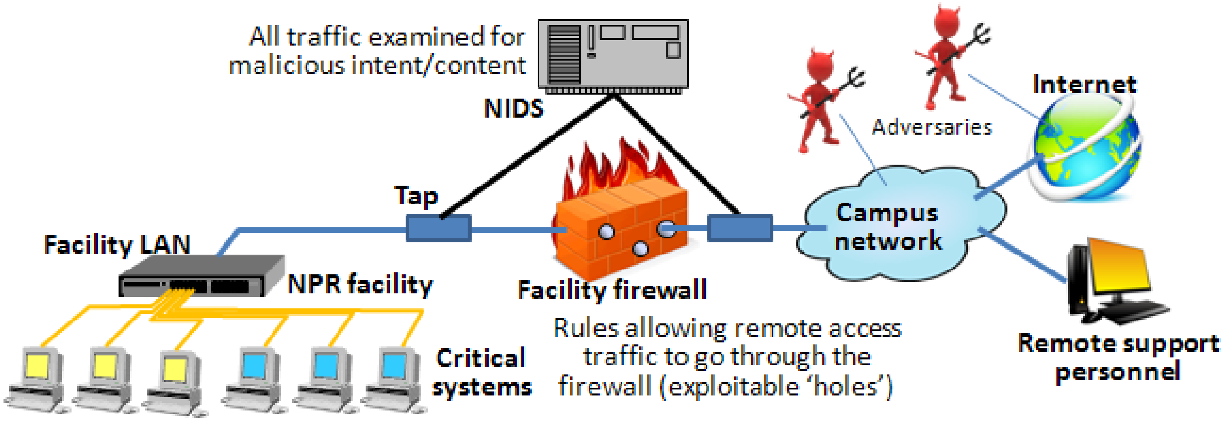


Figure 6.15 – Installing a NIDS to inspect all NPR facility message traffic

A NIDS is software (and supporting hardware) that would examine every message packet as they attempt to enter or leave the NPR facility LAN and would look for known message content and message patterns/sequences that are indicative of malware, of cyber reconnaissance activities and of actual cyber attacks. Figure 6.15 shows how a NIDS could be positioned around the NPR facility firewall to see all message traffic both incoming and out-going, including traffic the firewall blocks. Some university IT departments may already have a NIDS in place to monitor traffic entering and exiting the university's network. In that case it may be possible to merely add additional NIDS sensors and network taps (devices that allow Ethernet message frames to be 'copied' for the NIDS) around the NPR facility firewall and have the existing NIDS monitor that specific message traffic.

Section 7: System administration and support issues

Almost all digital systems and devices (including CDAs) have some level of initial configuration that must be done to commission them and many also require periodic configuration modification activities (e.g., updating firewall rules, enrolling new personnel into an access-control system database or biometric scanner). The term “administration” is often used to encompass all such activities. (This is different from repair and maintenance activities.) Some devices and systems may also require maintenance activities as well, either periodically (e.g., replacing internal batteries annually) or as-required due to damage, faults or failures. In the case of both maintenance and administrative activities, there is a potential risk of unauthorized and potentially malicious manipulation or alteration of settings, data, or even software to defeat or degrade the function and effectiveness of the systems/devices. For an NPR facility, this is particularly an issue as regards the physical access control and intrusion detection systems because defeating these systems would be important to an adversary seeking to steal nuclear materials.

Maintaining a CDA Inventory– A basic requirement for ensuring that you maintain adequate cyber security on your facility CDAs is to maintain an accurate and complete list of those systems and devices deemed to be CDAs (per the Table 4.2 criteria). In addition you want to be able to restore or replace the CDA if it is damaged or fails and to ensure your ability to do this, for each CDA, you ought to maintain up to date records of cyber security and configuration related information and restoration materials.

EP#44 – An effective cyber security practice is to develop and maintain an up-to-date list of information and applicable materials for each identified CDA within the NPR facility, including:

- *The current inventory of software running on the system/device with version number of each*
- *The Manufacturer's model/serial number information for the CDA*
- *The list of security patches and/or software updates installed*
- *Installation disks/media for all installed software*
- *The licensee key (if any) that activates/enables the software in case it must be reinstalled*
- *Backup media that can be used to restore the current configuration of the CDA (where applicable)*
- *Written procedures for performing a backup or system restore (where applicable) for the CDA*
- *An inventory of any special items (dongles, keys, media drive, etc.) required to perform a backup or restoration of a CDA, including their location and person responsible for their custody*
- *A list of all personnel with accounts/user IDs on the CDA, especially any with administrative/root access rights*
- *A list of any passwords required to enable/use/operate the CDA. This list should be kept in a secure manner, preferable encrypted and treated as being highly sensitive information*

Configuration versus programming - Some of the digital devices/systems used for access control, video surveillance, physical intrusion detection, as well as for reactor operation have all of their software/program code in ROM and thus their programming cannot be altered through any purely cyber means (physical access and physical tampering would be required). For these devices, the main threat is alteration of their configuration settings which, depending on the type of CDA and the specific setting, might drastically alter CDA functionality. Other devices have firmware in alterable memory (e.g., flash) and can receive firmware updates. These are thus potentially vulnerable to malicious firmware as well as to alteration of their configuration settings (although installing firmware updates would typically still require having physical access to the CDA). Still other devices/CDAs are (or contain) full-function computers running commercial operating systems and are thus vulnerable to software modification and a range of malware and attack exploits as well as to configuration modification, especially if they are network connected or make use of portable media for data/file exchanges.

Administrative access - CDA maintenance and repair functions, when needed, typically involve either having a vendor service representative come to the licensee’s site or having to send the broken equipment back to the vendor. The cyber security issues associated with maintenance and repair are a supply chain consideration and addressed in Section 11. The NRC staff determined that the routine CDA administrative and support functions were generally being performed in one (or more) of the following three ways:

- Local administration (within the facility by NPR staff/contractor)
- University-supported (by IT, locally and from across the university WAN)
- Vendor-supported (from across the Internet and university WAN or via a dial in/out connection into the wired/cellular public phone system)

The primary cyber security concern associated with CDA administration/support is the possibility of accidental or malicious setting changes that alter, degrade, or disable CDA functionality or the accidental or intentional introduction of malicious software or software changes into CDAs, where this is technically possible. When administration is done locally (the first bullet above), the process can be managed and overseen by the NPR staff even if a contractor is brought in for that purpose. If a CDA is isolated then local administration is the only possibility. Even if the CDA is connected to an isolated LAN within the NPR facility, local administration is still the only possibility, although this opens up the option of administration from across the isolated LAN.

Local administration- For CDAs that are actually multi-user computers administration can usually be performed via the human-machine interface (HMI, i.e., keyboard, mouse, and display) given the necessary user account privileges (and account password). Since improper administrative changes can degrade a

CDA's functions or even render it inoperative, administrative access should not be given to those without both the proper training/experience and the need for such access rights.

EP#45 – An effective cyber security practice is to restrict the number of personnel granted administrative (a.k.a. "super-user" or "root") rights/accounts on each CDA and to ensure that all such personnel have applicable training and experience in administrative functions for the CDAs on which such rights have been granted.

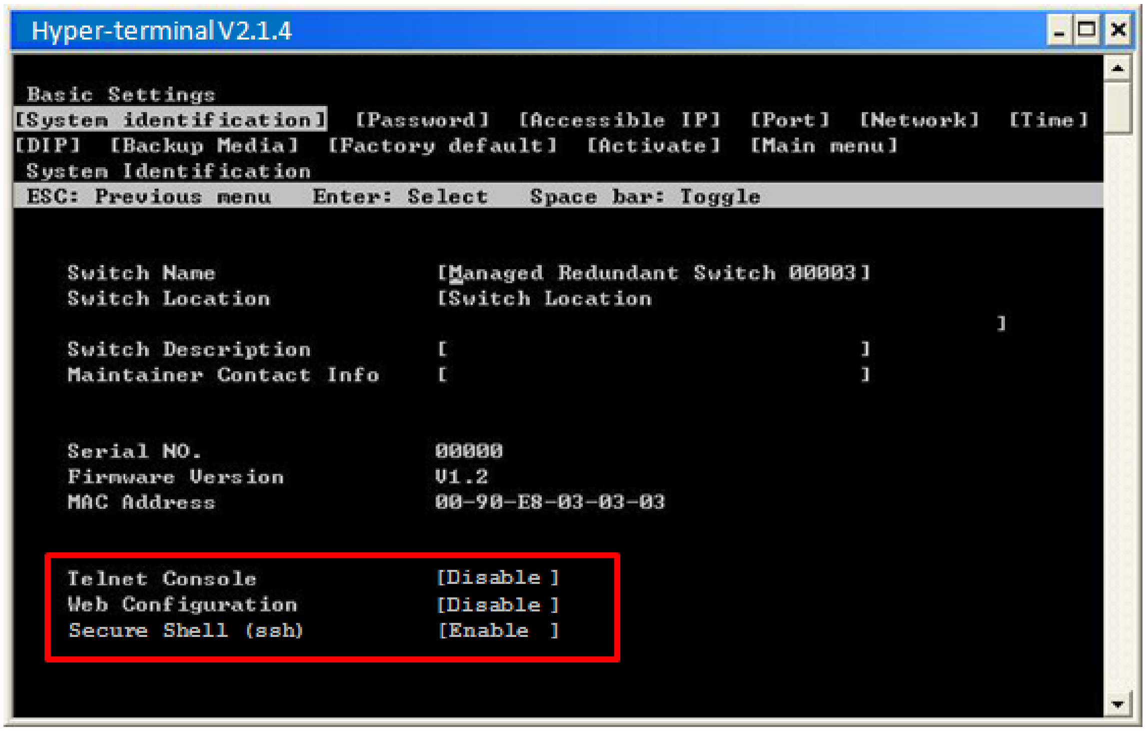
Many lower-functionality CDAs (e.g., a digital trend recorder) may either provide some level of administrative access via their HMI (possibly in the form of a menu system) or may support some form of user interface program that has to be accessed using a separate (laptop) computer and use either a console port or an Ethernet connection. Figure 7.1 is an example of a user interface accessed via a laptop PC connected to the CDA's console port using a program (such as HyperTerminal©) that emulates a dumb ASCII terminal.

Network-based administration- Today, many CDAs (even low-functionality ones) support Ethernet-IP network communications for administration and configuration. Using these capabilities may involve making a direct Ethernet connection from a PC/laptop to the CDA or attaching the CDA to a common LAN (e.g., connecting it to a shared Ethernet switch). Some CDAs will "wake up" with default IP settings which enable communications (and alteration of those default settings). Some CDAs may also have a dedicated local, non-Ethernet "console" port that can be used to configure the CDA and setup its networking functions (e.g., assign it an IP address and subnet mask). Many CDAs with Ethernet-IP networking capabilities come with vendor-default configuration settings that are not cyber secure, and which need to be changed prior to putting the CDA into service. An example is given below in Figure 7.1 where the CDA (an Ethernet switch in this case) comes with telnet, secure shell (SSH), and hypertext transfer protocol (HTTP) communication connectivity enabled (see the red box on Figure 7.1). If the CDA is to be isolated its console port (if it supports one) can be used for local administration and none of the remote connectivity options would need to be enabled.

EP#46 – An effective cyber security practice is to disable CDA communication functions that are not required to eliminate potential attack pathways into CDAs and to utilize local CDA ‘console’ ports for administration where possible, rather than performing cross-network administration of the CDA.

In this particular example (Figure 7.1), the CDA will be administered across an NPR facility isolated LAN so at least one of the remote Ethernet-IP communication facilities needs to be enabled. Since SSH is the only one of the available choices that uses encryption and authentication, that is the obvious choice and the only remote access function that will (should) be enabled on the CDA.

EP#47 – Where a CDA must be administered across a network an effective cyber security practice is to only make use of encrypted/authenticated remote access functionality such as SSH and HTTPS (encrypted HTTP) and to assign each CDA a strong (long/complex), unique password.



```
 Basic Settings
[System identification]  [Password]  [Accessible IP]  [Port]  [Network]  [Time]
[DIP]  [Backup Media]  [Factory default]  [Activate]  [Main menu]
 System Identification
 ESC: Previous menu    Enter: Select    Space bar: Toggle


    Switch Name                  [Managed Redundant Switch 00003]
    Switch Location              [Switch Location
                                                                ]
    Switch Description           [                              ]
    Maintainer Contact Info      [                              ]


    Serial NO.                   00000
    Firmware Version             V1.2
    MAC Address                  00-90-E8-03-03-03


    Telnet Console               [Disable ]
    Web Configuration            [Disable ]
    Secure Shell (ssh)           [Enable  ]
```

Figure 7.1 - Default network settings configured via the CDA's console port

Remote access- The primary concern with permitting remote/cross-network administration of CDAs (the second and third bullets above) is that this requires enabling support capabilities on the CDA (e.g., enable telnet, ssh, http, etc. as shown in Figure 7.1) and, if done from outside the NPR facility, allowing corresponding message traffic through intervening firewalls. Skilled hackers are able to infer firewall rules through traffic analysis and find ways to use these security holes to attack and compromise the CDAs. Figure 7.2 shows the three basic administrative options: direct connection to the CDA, network-based administration via the NPR's (possibly isolated) LAN, and network-based administration from across an external network (possibly including the Internet).

The greatest threat comes from permitting administration from across an external network. However, there are measures that can be taken to make such occasional remote access much more secure and less likely to provide an adversary with an exploitable vulnerability.

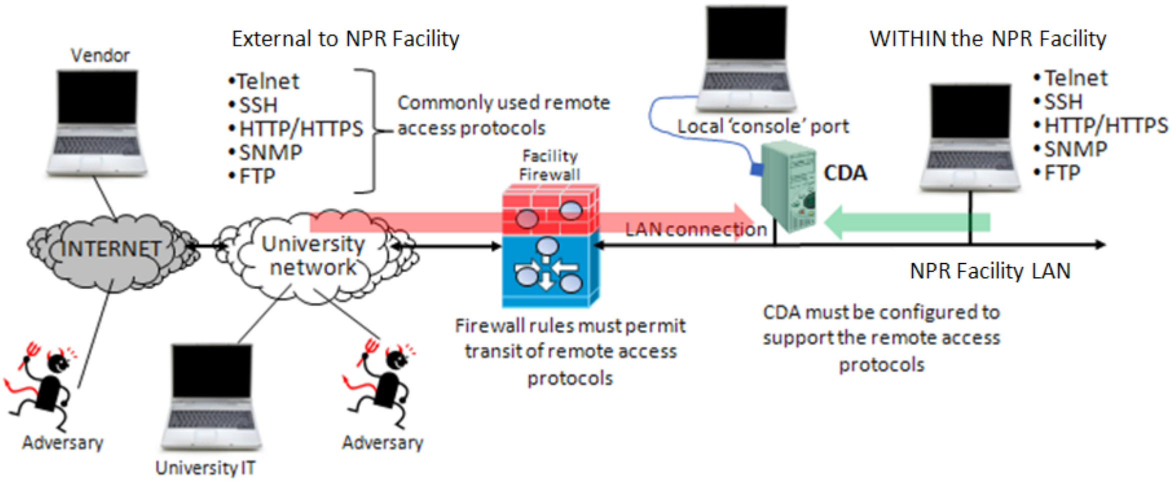


Figure 7.2 – Local administration, local via LAN and remote via WAN

Another type of VPN - If a given CDA/system is going to regularly require remote (cross-network) administrative access, whether by university IT personnel, vendor personnel, or both then it may make sense to configure VPN access. In Section 6, the concept of a permanent site-to-site VPN was discussed for securing surveillance video and the issue of site-to-site cross contamination was raised. For remote, occasional, cross-network secure administrative access a different type of VPN is best: a mobile VPN client. In this approach one or more designated laptop PCs to be used for remote administration are configured with VPN client software and the firewall at the NPR facility (or a separate VPN server) would need to be configured with matching VPN server software. For a VPN client to be accepted/authenticated by a VPN server, the client needs to be issued a digital certificate. Digital certificates can be purchased on-line (by the NPR facility or university IT department) from any number of sources (or self-issued by the university IT department given the necessary software) and emailed to the organization that is to provide administrative support (who will then load that cert onto their designated laptop). Digital certificates contain encryption keys for authentication and message encryption as well as a defined start/stop validity date (set by the issuer per the requirements of the purchaser) that can be used to limit the time window available for having remote access. Once the cert expires, the remote access will no longer be allowed; at least until a new cert is issued and loaded into the laptop. Running a VPN server in a firewall eliminates the need for firewall rules that create exploitable vulnerabilities.

> *EP#48 – Using mobile client VPNs with temporary (short-duration validity) digital certificates issued to the support organization by the NPR is an effective cyber security means for limiting and managing remote administrative access into CDAs and for eliminating the need to have firewalls with exploitable remote-access security holes.*

Non-networked remote access- Remote, temporary administrative access to CDAs (or onto an isolated LAN) can also be established in ways that avoid traversing the Internet and the university WAN. The particular approach will depend on a range of technical issues (such as does the CDA have a console port?) But some methods that might be possible include the following:

1. Using dial in/out analog phone lines and modems
2. Attaching a modem-equipped router to an isolated LAN
3. Attaching a cellular gateway to an isolated LAN

Figure 7.3 shows all three methods at once (strictly for illustrative purposes). If a CDA has a console port that is in fact EIA/TIA-232 compatible, then it should be possible to attach a conventional analog, auto-answer telephone modem to the console port and to an analog (public, switched telephone network or PSTN) phone line and have a remote administrator establish a dial-in phone connection.

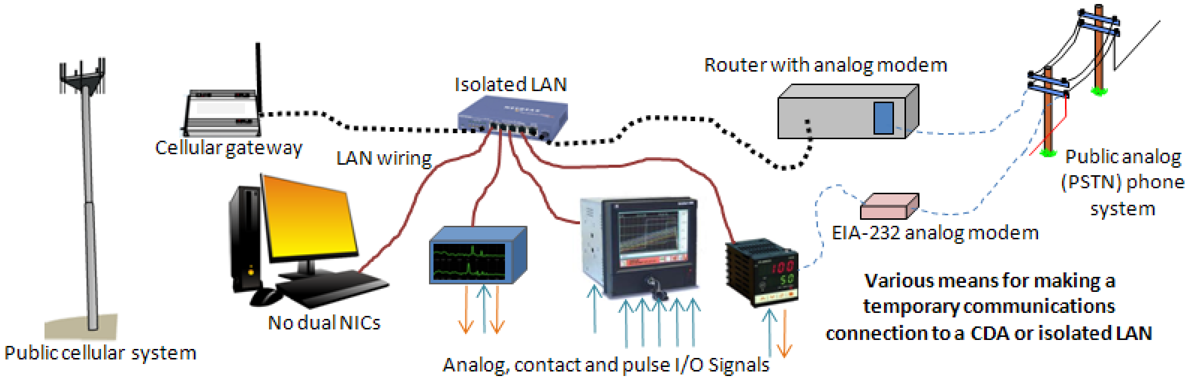
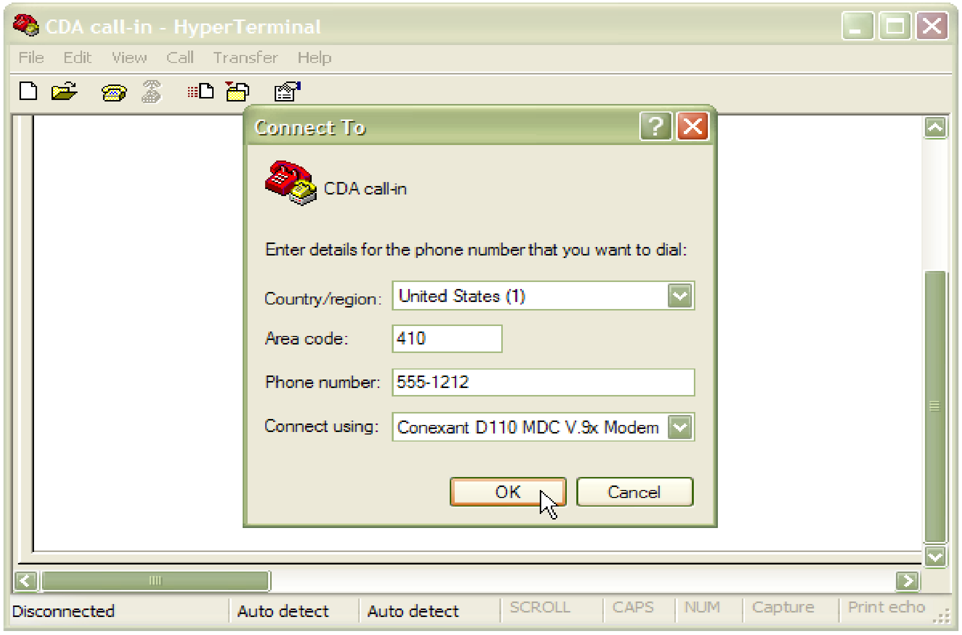

Router with analog modem
Isolated LAN
Cellular gateway
LAN wiring
Public analog (PSTN) phone system
EIA-232 analog modem
Various means for making a temporary communications connection to a CDA or isolated LAN
No dual NICs
Public cellular system
Analog, contact and pulse I/O Signals

Figure 7.3 – Establishing direct remote access to CDAs and isolated LANs

Various commercially available utility programs for different PC operating systems (such as Microsoft's HyperTerminal©) support making dial-up serial connections via the PSTN using either an internal or external modem. Figure 7.4 illustrates using the Windows HyperTerminal program to setup a telephone connection to a CDA with an auto-answer modem connected to an analog phone line with the telephone number specified in the "Connect To" panel.



Enter details for the phone number that you want to dial:

Country/region: United States (1)

Area code: 410

Phone number: 555-1212

Connect using: Conexant D110 MDC V.9x Modem

Figure 7.4 – Establishing a dial-up telephone connection via the PSTN

Since anyone could potentially dial into the CDA and make changes, were the phone line/modem left connected, it is essential to ensure that this cannot occur.

EP#49 – An effective cyber security practice is to have procedures to ensure that telephone modems and phone lines used for temporary remote access are disconnected and removed once the administrative activity is completed and are never left connected overnight, over a weekend or holiday or outside of normal working hours.

If multiple CDAs are connected to an isolated LAN and support network-based administrative access, then it may be possible to attach a router that incorporates an analog telephone modem to the isolated LAN and to an analog phone line. Again, this would enable a remote dial-in phone connection but the connection would use the PPP (point-to-point protocol) IP link layer protocol and the caller's message traffic would be routed onto the isolated LAN, giving them access to any/all of the CDAs. Again, it would be very important to ensure that the analog phone line is disconnected once remote administrative activities are completed and never left connected overnight, over a weekend or holiday or outside of normal work hours. There are also technology choices (cellular modems and router/gateways) that allow for dial-up connection through the cellular phone system rather than the wired/analog phone system. But be careful as some cellular gateways route traffic directly onto the Internet, which you are specifically attempting to avoid by using these remote access methods.

Additional recommendations- With any form of remote access, there are additional steps, beyond just disconnecting temporary equipment and phone connections, which should be taken to minimize the possibility of such access being exploited.

Section 7: System administration and support issues

EP#50 – Effective cyber security practices for managing remote administrative access to CDAs also includes:

1. *Creating a temporary administrative user account on the CDA and have the remote personnel make use of that account. Once the support activity is completed the temporary account can be deleted from the CDA.*
2. *Some CDAs do not have individual user accounts, only a single password that is used universally by all users. In those cases change the actual CDA password to something different (anything) and provide it to the remote personnel. Once support is concluded change the CDA password back to the actual value.*
3. *If the support activities will involve updating firmware or installing patches or software updates then prior to the support, if possible, make a backup of the existing CDA firmware/software so that changes can be reversed if necessary.*
4. *If support activities involve making configuration/setting changes, review and document the changes that will be made in advance and then verify that only those changes were made once the support activity is completed. Keep track of previous settings in case it turns out that the changes implemented have an adverse impact and need to be un-done.*
5. *Always maintain documentation that lists the current valid configuration settings for all of your CDAs.*
6. *For some CDAs (those based on computers running a COTS operating system) it may be possible for malware to spread to the CDA from an infected computer used for remote administration. All such CDAs should be running a host-based (personal) firewall or HIDS that will block attempts to install malware or to access/exploit vulnerable ports and services.*
7. *PC/Computers used for remote administration, if used for any other purposes and/or connected to a corporate/university WAN or the Internet, should be hardened, have a HIDS installed and be AV scanned before use for CDA remote support.*

Section 8: Personnel cyber security training issues

Staff cyber security training - In many cases, the effectiveness of technical cyber security measures (and even physical security measures) can be significantly degraded because of the actions (or inaction) of site personnel, often because of a lack of training and familiarization with applicable cyber security processes and procedures. Two of the leading means used by hackers to break into well-protected systems are to trick personnel into opening infected email attachments and into visiting malicious web sites (by clicking on a hyperlink). Strictly technical measures cannot prevent such actions; the best means of prevention is to educate personnel about the dangers and the social engineering tricks involved. At the sites surveyed the cyber security knowledge and awareness of the staff varied greatly. None of the licensees surveyed had formal programs aimed at providing all of the NPR permanent staff (or students, contractors, and research personnel) with some basic cyber security training and awareness. Since the inadvertent and misguided actions of personnel can have a major impact on cyber security adequate and applicable training is important.

EP#51 – An effective cyber security practice is to ensure that all NPR personnel receive a basic introduction to the topic and that personnel performing administrative functions and/or utilizing CDAs receive an additional level of cyber security training.

Some of the most essential topics of cyber security awareness and training for all personnel working at the NPR facility include the following:

- Threat actors and their motivations
- Safe web browsing/surfing
- Social media do's and don'ts
- Safe email practices
- Password policies
- Use of portable media
- Use of portable electronic devices

- Use of wireless networks
- Awareness of social engineering tactics and methods
- Protecting user credentials
- Incident response and reporting

In addition to basic cyber security awareness training, it is important that applicable NPR personnel be cognizant of relevant university and NPR cyber security policies and procedures.

EP#52 – An effective cyber security practice to ensure that all NPR personnel, and those working with digital systems and assets at the NPR facility, should be made aware of existing university/organizational IT policies and procedures related to their job activities.

For NPR personnel, or contractors, who will be supporting CDAs and be granted administrative (a.k.a. “root”) access rights on all/some CDAs, it is important to have an additional level of cyber security training since such personnel could potentially do more unintentional damage to CDAs because of their access rights. Although some of the training would be system/CDA-specific, a general set of topics for such personnel could include the following:

- Account management
- Activity logging
- Making and maintaining backups
- Essential operating system policy settings
- Scanning portable media
- Installing patches and updates
- Installing new applications
- Personal firewall usage/configuration
- Essential network configuration settings

Continuous monitoring of cyber risks – The cyber security threat landscape is constantly changing and evolving. New vulnerabilities are discovered and published daily, and new threats and risks are identified regularly by industry and cyber security research organizations. Ensuring cyber security measures retain their effectiveness requires awareness of developing trends in cyber security. Government organizations like the Department of Homeland Security's (DHS) U.S. Computer Emergency Readiness Team (US CERT) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) operate mailing lists for providing timely cyber security issues, vulnerabilities and exploits. Other commercial security information sources like the SANS Internet Storm Center, Symantec's Buqtraq, Secunia Advisories, and the SecLists.org Full Disclosure mailing list also provide valuable information regarding emerging threats, vulnerabilities, and research. Individuals responsible for overall cyber security at NPR facilities should avail themselves of these resources whenever possible to effectively evaluate the facility's risk profile.

EP#53 – An effective cyber security practice is for administrative personnel with cyber security responsibilities to subscribe to one or more cyber security advisory services to receive up-to-date information on new cyber threats, attacks, exploits, and vulnerabilities.

Factory-default configuration settings- Most digital devices, from PCs to Ethernet switches and even firewalls, are setup at the factory with default configuration values that are aimed at ensuring at least basic functionality out of the box if the device is used by someone with no IT experience or expertise. The problem with this is that it can give the illusion of proper and secure operation while the reality is quite the opposite. The default settings are in fact usually the most liberal (e.g., allow everything) and least cyber secure (e.g., no password required).

EP#54 – An effective cyber security practice is to ensure that ALL computer-based devices and equipment is put through an initial deployment review where factory default configuration settings are inspected and modified, as needed, to align with the security requirements and policies of the RTR facility and/or the University/organization, and to eliminate obviously insecure settings and configuration defaults.

Section 9: Use of portable media and portable digital devices

As has been mentioned in Section 6, one way for malware to make its way onto isolated devices and systems is through the incautious use of portable, removable, computer-readable media (passive portable media or PPM) and via portable/mobile electronic devices (PMD) capable of file storage and communications. Both PPM and PMD have a high potential to be a delivery mechanism for viruses, malware, and other malicious code, and care should be exercised, especially when the portable media was created or used on other, non-secure networks and computers.

Sensitive information transfers - Portable media may also be used to move files, data, and other information between and among systems and devices. If the information placed onto portable media is SGI or classified, then the information should be encrypted on the originating system prior to placing it onto the portable media and decrypted on the receiving system. This will reduce the likelihood of that information being disclosed were the portable media to end up in the wrong hands.

EP#55 – An effective cyber security practice is to use passive media for the transfer or sensitive information, to employ strong encryption with a complex shared key to secure the information and to ensure that the media is either stored or destroyed in an adequate manner once the transfer has occurred.

Potentially dangerous portable electronic devices obviously include laptop PCs, but actually numerous USB-connected devices such as MP3 players, digital cameras, and even color printers and scanners can be used to deliver malware. During the survey of NPRs it was noted that few licensees had policies or procedures in place to prevent the spread of malware via portable media and portable devices. Figure 9.1 shows how the use of these items on systems connected to the facility LAN as well as on critical digital assets creates the potential for infections to jump to supposedly isolated assets.

Section 9: Use of portable media and portable digital devices

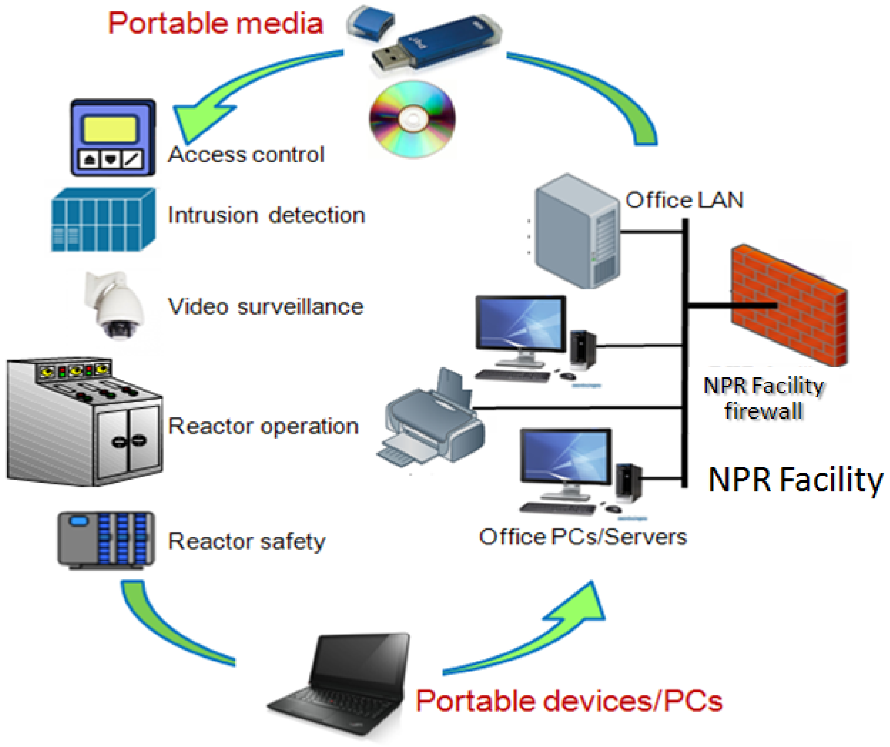
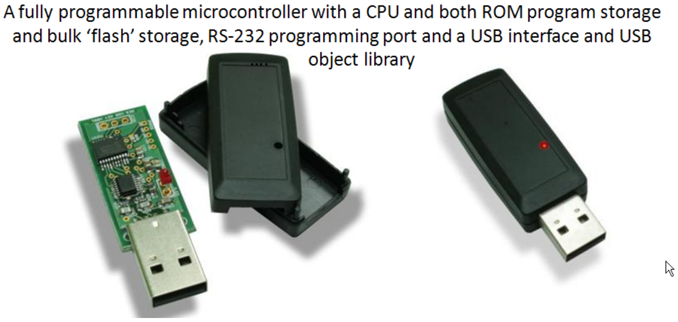


Figure 9.1 – Migration of malware between assets on PM/PD

Different types of portable media - Portable media (things used to transport files/data/software between computer devices and systems) includes both passive media as well as active media.

Passive media is media without any microprocessor circuitry or firmware and includes such things as magnetic tape, floppy disks, CD/DVD platters, memory sticks (Sony), CompactFlash cards SanDisk and SD (secure digital card). The primary risk posed by passive media is the contents of the "data container," the area of the media that contains computer-readable files.

Active media includes devices that contain a data container as well as an actual microprocessor and software. Active media interacts and interfaces with other computers via a communications port. This would include most USB connected devices such as thumb drives and external disk drives. Such devices may have the ability to obfuscate their contents through the use of encryption or by hiding the presence of specific files. Some such devices (specifically USB peripherals such as the one shown in Figure 9.2) can actually be programmed to spoof/fool the systems to which they are connected into believing them to be a range of peripheral devices and using this capability to send malicious commands and software into the systems. A USB connected device plugged into a PC is essentially an independent computer that is using the USB channel to communicate with applications running on the PC. Those PC applications rely on the assumption that the software running on the USB device is non-malicious. Just as in passive media, the data container of active media poses a risk in that it may contain malware. However, the underlying computing and processing capabilities of active media pose an additional risk which must also be considered.



A fully programmable microcontroller with a CPU and both ROM program storage and bulk ‘flash’ storage, RS-232 programming port and a USB interface and USB object library

Figure 9.2 – Programmable USB “dongle” with integral microcontroller

Whether active media or passive media is used to transfer information to a system, the contents of the data container on the media can be a vehicle for viruses, malware, or other malicious code. Whenever introducing information into a critical network/system using media and files from an external source, there is always a risk of infection.

EP#56 – An effective cyber security practice, when loading or copying information/files/data onto a critical system or CDA is to first perform an anti-virus scan of the media used for the transfer, and its contents, on a separate system designated and configured for that purpose.

Section 9: Use of portable media and portable digital devices

A USB-connected device can contain data and files (and even functionality) that are invisible to an AV scanning program running on a PC since the software of the USB device totally controls what is made available to that scanning software. For the same reason, it is not possible to be absolutely sure that erasing the contents of such a device actually results in full erasure since, just as such a device can hide files from a scanner program, it can also merely pretend to erase files when asked to do so (or just ignore such requests).

EP#57 – An effective cyber security practice, when moving information/files/data between systems (particularly critical systems) on portable media, is to only utilize passive media (e.g., a CD or DVD) for such transfers, if possible.

Using passive media for file/information exchange with CDAs is not the only step that should be taken, but it is an important one. Of course not all devices/systems support passive media (in fact many tablet PCs only support USB for information exchange) and so it may be necessary to use active media (e.g., a USB thumb drive) for such transfers. If this is the case, then it is important to use USB bulk-storage devices that are physically controlled and managed.

EP#58 – An effective cyber security practice is never inserting/connecting an unknown USB storage device into a critical system/CDA. It is recommended that one purchase a set of 'dumb' flash/thumb drives (ones with no encryption capability), label them as being exclusively for use with CDAs, and then fully erase and AV scan all of them (on a non-critical system/computer) prior to using them with any of the CDAs.

The use of dedicated, pre-scanned, and validated active media that is dedicated for use only on the RTR network and associated computers will reduce the risk of infection of either the data container or the underlying software and firmware. However, the portability of these devices makes it easy to transport into and out of the controlled areas either intentionally or unintentionally. Once out of the controlled environment, they can easily be lost, stolen, accidentally used for other purposes, or used in other environments.

EP#59 – An effective security practice is to clearly mark and label (or even color-code) active media devices assigned for use on critical systems/CDAs, as well as implementing reasonable positive-control measures to reduce the risk of intentional or accidental cross-contamination from unauthorized media.

USB connected devices with mass storage– There are a number of digital devices that contain files systems that can be accessed via a USB connection: MP3 players, digital cameras, cell phones, and even many printers. When connected to a PC via USB they advertise their mass storage functionality and the PC loads the applicable driver and mounts their file system for reading and writing. Figure 9.3 shows examples of some typical USB mass storage devices.

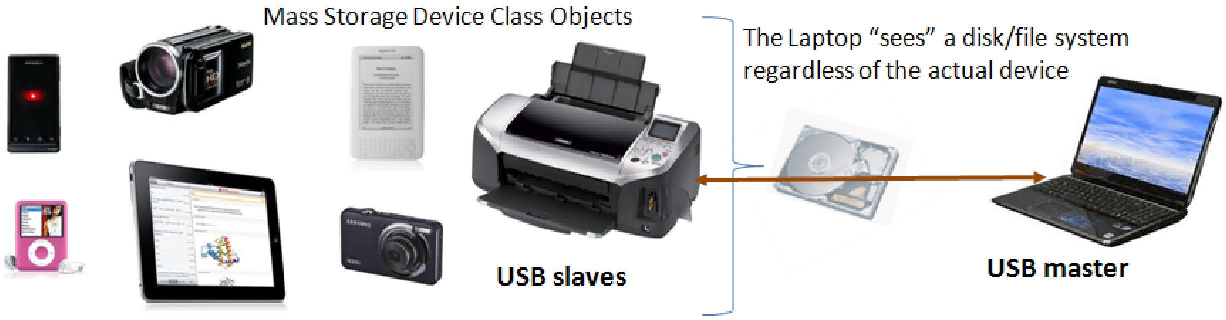

Mass Storage Device Class Objects
The Laptop "sees" a disk/file system regardless of the actual device
USB slaves
USB master

Figure 9.3 – Digital devices supporting USB accessible file systems

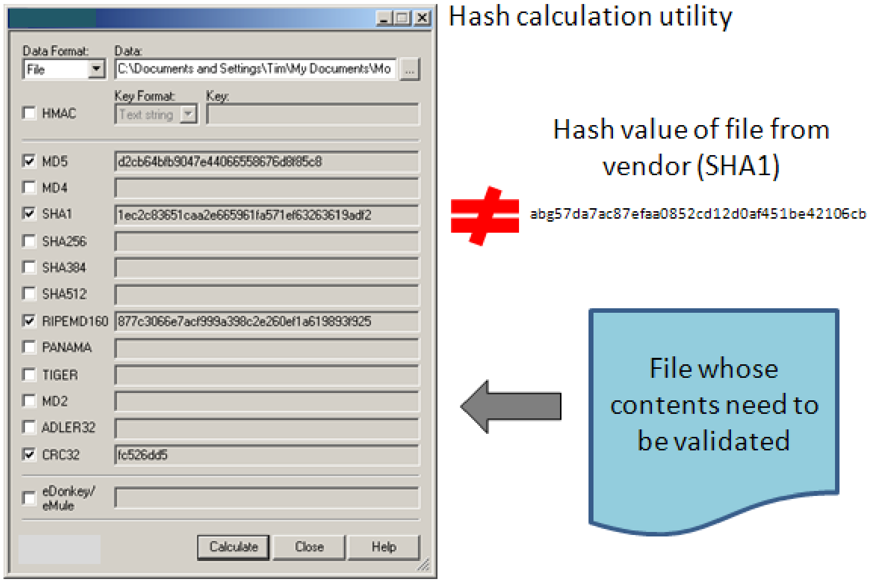
This means that these sorts of devices can be used to both carry the kinds of files for which they were intended (e.g., image files in a digital camera and audio files in an MP3 player), but most can also be used to carry any kind of file including files containing malware. Some printers incorporate a slot (or slots) for inserting portable media so that files can be printed without needing to have a PC. This means that such a printer, although benign itself, can provide a pathway for infected portable media. If such a printer has a USB connection to a computer and media is inserted, that media becomes available/visible to the computer as a mass storage object.

EP#60 – An effective cyber security practice is to never connect portable digital devices to CDAs via USB without first running an AV scan on their file system (possibly by connecting them to a separate computer designated and configured for this purpose.)

EP#61 – An effective cyber security practice is to never insert portable media into the media slots on printers connected to CDAs via USB, or shared by CDAs via a common LAN, unless the media has previously been AV scanned on a separate system.

Hash codes to detect tampering- When vendors provide files with software/firmware updates and revisions, especially where you download them from the vendor's website, it is becoming more common for vendors to also publish a "hash code" for the individual files so that you can verify that the files have not been damaged or intentionally altered (such as by being infected with a virus). A hash code is a numeric value generated by putting the file through a series of operations that produce a unique resulting value (any change in the file, even just altering one bit, will produce a drastically different hash value). There are a number of hash code algorithms used although the message digest (MD) and secure hash algorithm (SHA) versions tend to be the most common. There are web sites that will generate hash code values for you if you upload your file. There are also many free hash code calculating tools. If you download a file and generate the applicable hash code value and then compare it to the hash code provided by the vendor, you can be assured that the file retains its integrity (hasn't been altered) if the published hash code and the value you computed match. Figure 9.4 shows a typical has code generating applications and the various hash algorithms that can be used.

EP#62 – An effective cyber security practice is to make use of hash codes to verify the integrity of files before their content is presumed to be trustworthy and to verify that files have not been tampered with or replaced with malicious content. In addition it is an effective practice to generate and record/provide hash codes for files being exchanged with other parties (whether sending or receiving), regardless of the files' contents/type (software, data, images, video, applications, etc.) on a separate system.



Data Format: File
Data: C:\Documents and Settings\Tim\My Documents\Mo
□ HMAC Key Format: Text string Key:
☑ MD5 d2cb64bfb9047e44066558676d8f85c8
□ MD4
☑ SHA1 1ec2c83651caa2e665961fa571ef63263619adf2
□ SHA256
□ SHA384
□ SHA512
☑ RIPEMD160 877c3066e7acf999a398c2e260ef1a619893f925
□ PANAMA
□ TIGER
□ MD2
□ ADLER32
☑ CRC32 fc526dd5
□ eDonkey/eMule

Calculate
Close
Help
Hash calculation utility
Hash value of file from vendor (SHA1)
≠
abg57da7ac87efaa0852cd12d0af451be42106cb
File whose contents need to be validated

Figure 9.4 – Using a hash code generation application to verify the integrity of a file

Where electronic versions of critical documents (such as material inventory or operational procedures) are being maintained, hash codes generated from known-good versions of those documents can be used to verify that such documents (or copies thereof) still retain their integrity.

Since hash codes are large binary numbers (up to 512 bits long), they are usually displayed or written as either hexadecimal values (base 16 – where each group of 4 bits are represented by the decimal digits of 0-9 and the letters A-F) or using base 64 encoding. In base 64 encoding groups of six bits are represented by the upper or lower case letters (a-z, A-Z), or decimal digits (0-9) or the characters "+" or "/".

Protecting portable computers– Portable computers (laptops, tablets, PDAs, etc.) that are used for supporting and managing CDAs need to be protected so that they don't end up being used to spread malware and as a platform for attacking CDAs. In Section 9, the issue of CDA administration was discussed and it was pointed out that portable computers are often used for CDA support, whether to run vendor-specific tools, exchange files, upload new firmware, or for administrative communications with CDAs. Since a portable computer could be highly susceptible to compromise and malware infection, it is recommended that measures are put into place to reduce this risk.

EP#63 – An effective practice to protect portable computers/devices used in support of CDAs or critical systems is to restrict such computers to the NPR facility, only connect those portable computers to critical systems/CDAs and isolated LANs within the NPR facility and NEVER use those portable computers to access any site/server/system on the Internet.

Therefore, when using a portable computer in outside environments (university network, home network, business network, etc.), it is recommended that the portable computer be configured to use the best possible protection methods against malicious network, software, or file activity. For laptops, this may be measures like installing a firewall program and an anti-virus scanning package. For handheld devices like PDAs and smart phones, this may be measures like implementing password protection and using an AV scanning app.

Section 10: Use of digital I&C technologies, including wireless versions

The manufacturers of commercial instrumentation and control devices have almost universally migrated onto smart (microprocessor-based) platforms and added both wired and wireless communications and advanced functionality to their product offerings. Many now also offer Ethernet-IP based network communications using one of the various “industrial protocols” (layer 7 – application layer protocols per the ISO/OSI reference model). This means that as NPR licensees need to replace or augment their reactor instrumentation and control equipment, it is probable that this will entail upgrading to the current commercially available product offerings with these sorts of capabilities.

Prior to the current general adoption of Ethernet as a LAN for instrumentation, several vendors and industry groups developed proprietary “fieldbus” LANs and many are still supported and readily available including the following:

- Foundation Fieldbus H1
- Profibus
- Interbus-S
- CANbus
- Datahighway/Datahighway+
- HART

Today most vendors have (also) aligned themselves with one or more of the Ethernet-IP based industrial protocol standards, including the following:

- Foundation Fieldbus HS
- ProfiNET
- EtherNET/IP + Common Industrial Protocol (CIP)
- Modbus/TCP
- EtherCAT

Wireless communications have also gained a lot of support and traction because of flexibility and lower installed cost and there are several competing wireless standards being used in industrial and commercial applications including the following:

- ISA 100.11.a
- WirelessHART
- ZigBee/XBee
- Vendor-proprietary
- WiFi WLANs

NOTE: In regards to smart instruments and control elements, it should be mentioned that the National Institute of Standards and Technology (NIST) has operating experience with smart instruments that shows that they have a significantly reduced usable lifespan (months versus years) when placed into service in areas where even a moderate level of radiation is present. So regardless of any cyber concerns about such devices, using smart instruments for NPR operation or safety may not be cost-effective or sufficiently reliable unless they can be adequately hardened or shielded.

Legacy Instrumentation bus – The instrumentation LANs (bus) that pre-date the conversion to Ethernet were/are proprietary and usually very limited in capacity (bandwidth) and geographic distribution (bus segment length). Most had a bus or trunk and drop design with a maximum length limit (up to 1000 meters was common) and the number of devices that could share any given bus segment was also limited (up to 32 devices was common). Connection of a computer to such a LAN required a special interface board/card (or a special gateway) and vendor-specific software. For all intents and purposes these could be considered as de facto isolated LANs and as long as proper physical security measures were implemented, the major cyber security consideration would be someone tampering with the configuration settings of the various devices/instruments. Figure 10.1 shows an example of a small, stand-alone control/automation system containing several instruments, controllers, and control elements as well as a full color, graphical HMI with a touch screen. The only true computers in this example are the rack-mounted HMI which runs a Windows XP operating system and the laptop PC (also running Windows) which has a LAN interface module (PCMCIA) and special software that allows it to act as a calibration and configuration device. In this example it also runs software for “programming” and downloading the PLCs (or creating a “programming” file for USB delivery). The configuration of graphical operator displays and database for the local HMI is often done off-line on a separate PC using the vendor’s software tools. Once the displays are developed, the configuration files are loaded onto the HMI via a USB thumb drive. In this example those software tools could also be running on the laptop PC. It is important to understand that the software tools for programming/configuring the HMI and PLCs (and the hand-held calibration tool) are all COTS (commercial off-the-shelf) products and so they are readily available to an adversary.

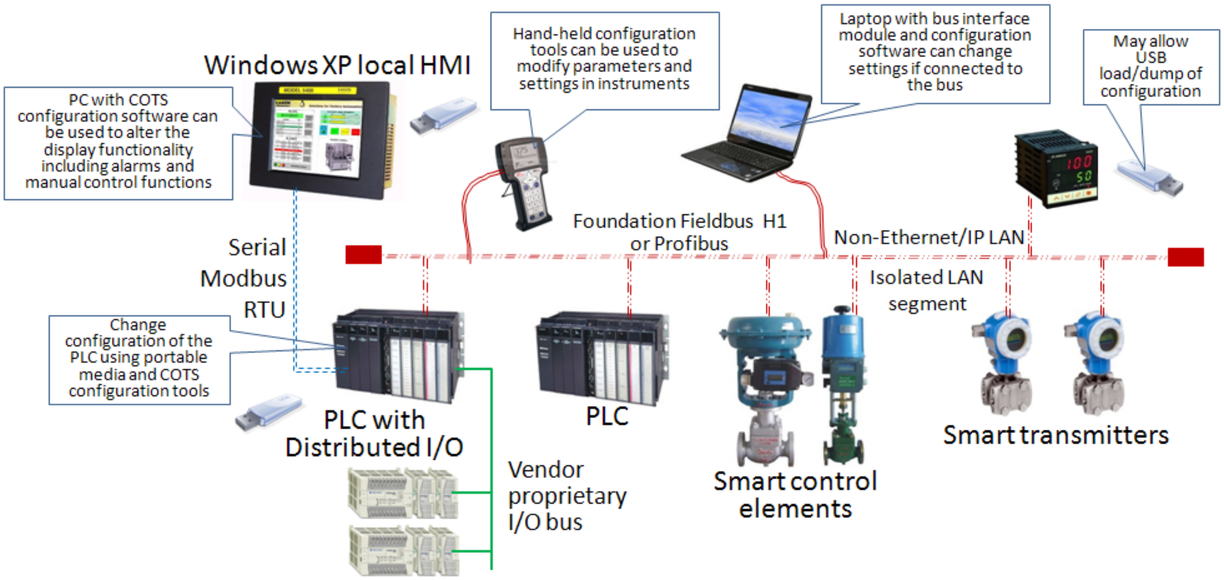

Windows XP local HMI
PC with COTS configuration software can be used to alter the display functionality including alarms and manual control functions
Hand-held configuration tools can be used to modify parameters and settings in instruments
Laptop with bus interface module and configuration software can change settings if connected to the bus
May allow USB load/dump of configuration
Foundation Fieldbus H1 or Profibus
Non-Ethernet/IP LAN
Isolated LAN segment
Serial Modbus RTU
Change configuration of the PLC using portable media and COTS configuration tools
PLC with Distributed I/O
PLC
Vendor proprietary I/O bus
Smart control elements
Smart transmitters

Figure 10.1 – An instrument bus can connect a range of smart devices

From a cyber security perspective, since an adversary would undoubtedly have access to all of the tools and software needed to compromise the various system components, the most effective cyber defense is to prevent them from gaining physical access to the system and to use/enable all available defensive capabilities of the components themselves (e.g., passwords). NPR facilities already have adequate perimeter physical security and access controls, but additional security measures can be taken to protect such a system.

EP#64 – Effective practices to protect bus/LAN-based smart instrumentation systems include:

- *Enclose all LAN media, junction boxes and access points in conduit and in locked enclosures*
- *Where possible, place system components into locked enclosures or rooms*
- *Use port locking/blocking devices (especially on USB ports)*
- *Use passwords/keylocks on devices that support them*
- *Perform hardening on all PC/computer components running a COTS operating system*
- *Use video surveillance to monitor physical access to key system components*
- *Do not leave configuration/programming tools connected to the system/LAN when not actively being used and keep them secured when not in use*
- *LAN access/connection points used for temporary connections (e.g., for the laptop PC and calibration tool) should be secured in locked enclosures*

One particular type of smart instrument that is often seen today is a hybrid device that is capable of producing a conventional analog (4-20 mA) signal but also of communicating over the same twisted pair of wires to calibration/configuration devices using HART (or Foundation Fieldbus) protocol. Figure 10.2 shows a simple 4-20 mA analog current loop consisting of a HART-compliant transmitter, an analog panel meter, and an analog input on a digital controller. A HART calibration unit can be attached to the loop and can communicate with the HART transmitter using tone signals, without impacting the concurrent operation of the analog current loop. In this configuration the HART transmitter is still outputting a 4-20 mA analog signal that represents the current value of the measured parameter. The HART calibrator allows a technician to adjust the scale of the transmitter, assign it a tag name and description and possibly set other configuration information. This can be done by connecting the calibrator at any point in the current loop wiring so the technician need not go to where the transmitter is located (although doing so is a common practice and most HART transmitters have a connector for this purpose).

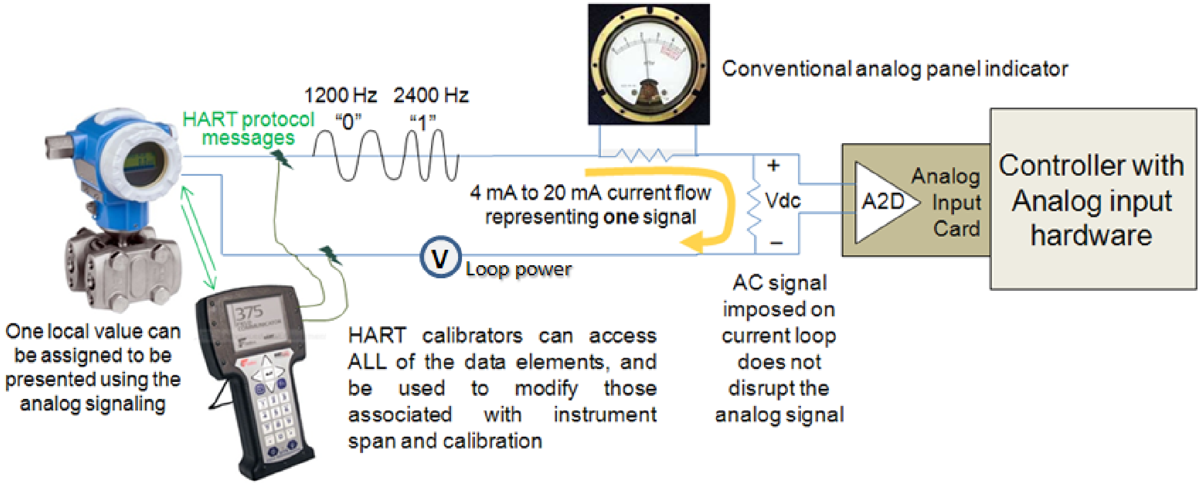

Conventional analog panel indicator
1200 Hz
2400 Hz
HART protocol messages
"0"
"1"
4 mA to 20 mA current flow representing one signal
+
Vdc
–
A2D
Analog Input Card
Controller with Analog input hardware
V
Loop power
AC signal imposed on current loop does not disrupt the analog signal
One local value can be assigned to be presented using the analog signaling
375
HART calibrators can access ALL of the data elements, and be used to modify those associated with instrument span and calibration

Figure 10.2 – A HART-compliant transmitter operating in analog mode

Used in this analog mode the other analog devices in the loop will not have access to any of this configuration information and cannot send messages to change any of the settings. But, using the calibrator device, it is possible (intentionally or accidentally) to cause the transmitter to generate invalid/inaccurate readings by improperly setting the scale configuration values.

EP#65 – An effective practice is to control access to all devices used for calibration and configuration, issue them only when needed and only to authorized personnel, secure them when not being used and have a second party confirm all changes made to calibration settings are correct and as approved.

Ethernet-IP based instrumentation fieldbus– Most vendors of wired instrumentation bus products have recognized the ubiquitous and low-cost nature and high speeds of Ethernet networks and have either created new versions of their products using one of the standard Industrial Ethernet protocols or have taken their own proprietary protocols and repackaged the messages and commands as data to be transported and delivered by TCP/IP or UDP/IP protocols as an OSI/ISO layer 7 (application) protocol. These protocols CAN co-exist on an Ethernet-IP network with other conventional protocols thus allowing a single, common LAN to be shared by business, office-automation, communications, security, and process control applications (a concept known as “network convergence”).

EP#66 – An effective cyber security practice is to keep CDAs on their own isolated LAN (see Section 6) or LAN segment (see Section 6) so that they are less vulnerable to cyber attack.

Since these instruments and control elements support an Ethernet NIC and a full five-layer IP communications stack, they are vulnerable to many of the network-based exploits that can be used to compromise computers/PCs and in fact they may be incapable of surviving a standard IT vulnerability scan. Most of these devices are not vulnerable to malware as again their program code is in ROM. But they, like the legacy instrumentation bus devices, are susceptible to configuration modifications. The most effective cyber defense for a system built using such devices is to prevent adversaries from gaining physical access to the system and to use/enable all available defensive capabilities of the components themselves. NPR facilities already have adequate perimeter physical security and access controls, but additional security measures (beyond LAN isolation/segmentation) can be taken specifically for such a system.

EP#67 – An effective cyber security practice for securing isolated Ethernet based instrumentation systems is to:

- *Enclose all LAN media, Ethernet switches, junction boxes and access points in conduit and in locked enclosures*
- *Where possible, place system components (CDAs) into locked enclosures*
- *Use port locking/blocking devices (especially on USB and Ethernet ports)*
- *Set passwords/keylocks on devices that support them, including Ethernet switches*
- *Utilize switch-based protective mechanisms such as MAC address locking ('port security') and administratively disable all unused ports*
- *Disable network-based switch administration support (e.g., telnet, ssh, http) and make use of the local console port for switch administration functions*
- *Perform hardening on all PC/computer components running a COTS operating system*
- *Use video surveillance to monitor/record physical access to key system components*
- *Do not leave configuration/programming tools connected to the system/LAN when not actively being used and keep them secured when not in use*
- *LAN access/connection points used for temporary connections (e.g., for the laptop PC and calibration tool) should be secured in locked enclosures*
- *Where possible, locked enclosures (and rooms) should have entry alarms wired into the physical intrusion detection system*

Wireless mesh networks – The various instrumentation vendors have also begun supporting the use of wireless networking as an alternate to wired instrumentation LANs. There are several competing wireless standards that are designed for secure and reliable operation in an industrial environment. It should be noted that the ISA (international society for automation) explicitly states that wireless communications are not to be used in any safety system or application. Only hard-wired communications should be used in those cases. There are several reasons for this but the primary one is that radio communications can be disrupted and blocked by many sources of RFI/EMF interference present in an industrial environment such as large electric motors, portable hand-held radios, and high-voltage electrical arcing. All of the wireless instrumentation standards operate in the unlicensed ISM (industrial, scientific and medical) radio frequency bands as do many other things like wireless Ethernet (WiFi), microwave ovens, cell phones, and cordless phones.

EP#68 – An effective cyber security practice is to prohibit the use of wireless instrumentation technologies in reactor safety applications.

Wireless instruments can be powered by internal batteries or from a power source. Battery power eliminates all wiring, but batteries need to be replaced periodically and have shortened lifetimes in very cold or hot environments. Battery powered instruments are not useful for measurements that must be read constantly and frequently as this rapidly draws-down the battery power. Most instrumentation experts suggest using wireless instrumentation in cases in which wires are not possible (e.g., a moving vehicle, rotating platform) and where the loss of the measurement would not create a dangerous condition or can be tolerated for an extended timeframe (e.g., level measurement in a reservoir/lake). They are also useful as a backup/alternative measurement source for a wired measurement. They can also be useful when a temporary measurement is needed as the deployment of a battery powered instrument can be done fairly quickly (but of course at least one central station [access point] must be deployed as well). Figure 10.3 shows how a wireless instrumentation mesh network can be created using one of the available standards, WirelessHART®. In all such WLANs access points and gateways must be powered; only the “end nodes” (the instruments and some control elements) can be battery operated. The ISA 100.11.a wireless instrumentation standard has a similar architecture but adds the ability to tunnel and gateway wireless devices that support other wireless standards. With these two standards, each node can provide message routing and forwarding services to enable point to point message exchanges.

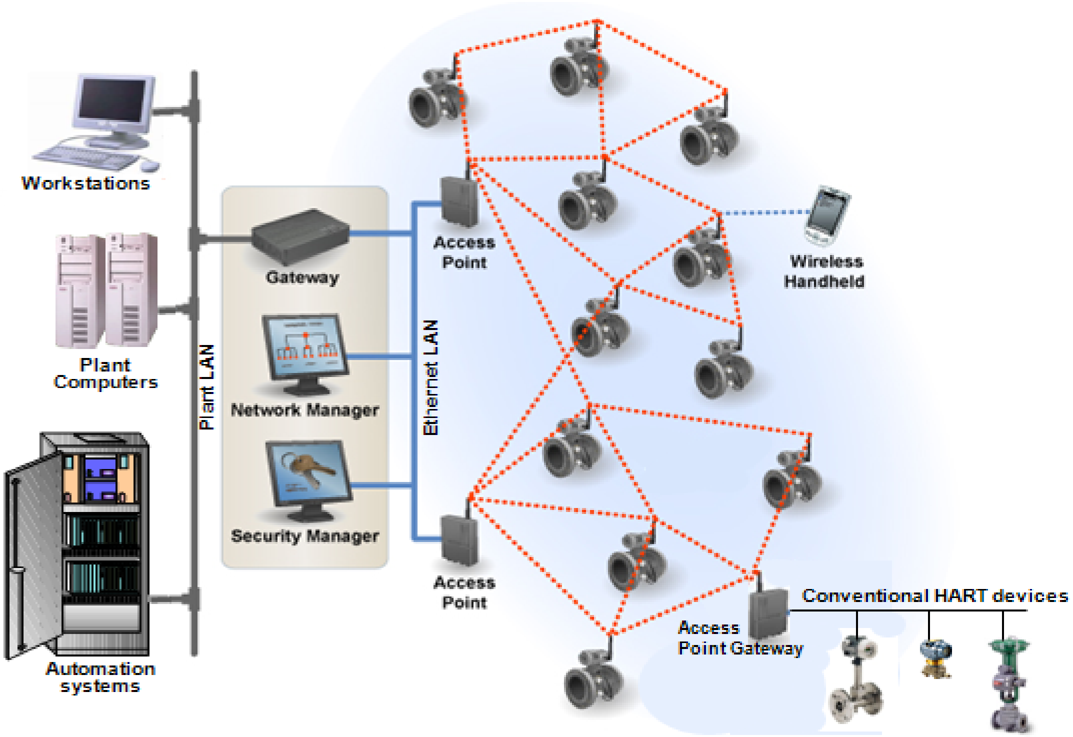


Figure 10.3 – A typical instrumentation WLAN based on WirelessHART

Most of the wireless instrumentation standards support a strong security model that incorporates encryption, authentication, and node enrollment as well as redundancy options for reliability. But these security services need to be enabled and configured.

EP#69 – An effective cyber security practice is to enable and utilize the security mechanisms available with wireless instrumentation standards.

Wireless commercial devices– Another wireless instrumentation standard based on the same basic low-power radio technology as used by wirelessHART and ISA 100.11.a is ZigBee. This technology is more focused on facility automation and commercial applications rather than plant/process automation but has gained reasonable traction in applications such as building automation and energy management. ZigBee (see Figure 10.4) was designed for applications with a lot of measurements spread out over a large geographic area, but where access to end devices (reading-from or writing-to) is infrequent so as to provide reasonable operational life for battery-powered end devices. ZigBee uses a centrally managed security model that supports key generation and exchange, encryption, and authentication services.

EP#70 – An effective practice when using wireless instrumentation is to restrict the use of ZigBee wireless technology to non-reactor (e.g., facility automation) applications.

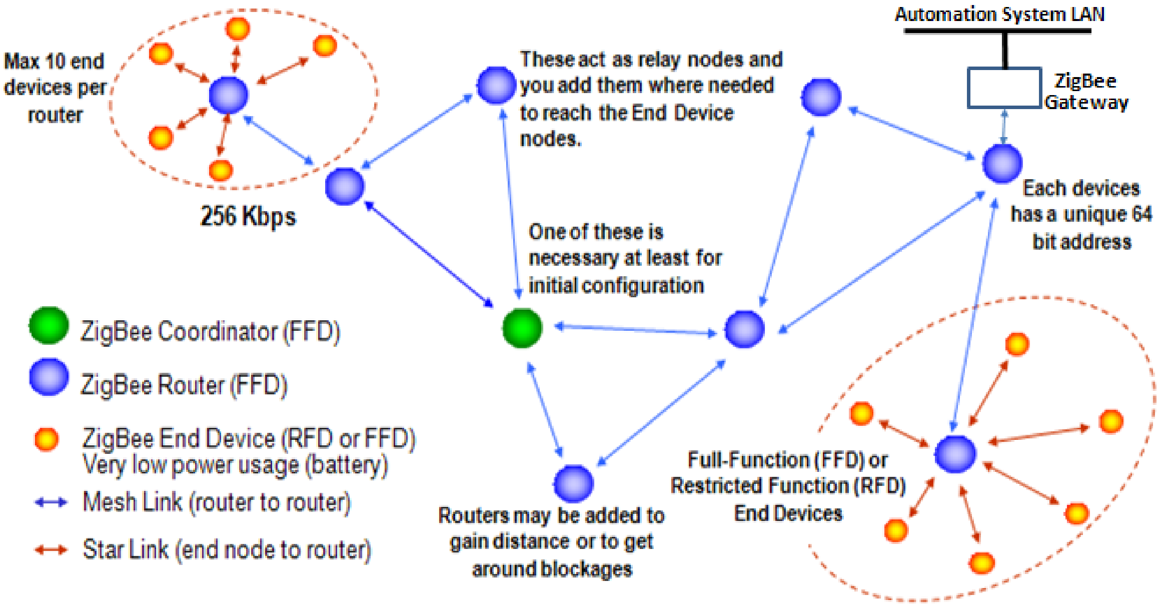

Automation System LAN
ZigBee Gateway
Max 10 end devices per router
256 Kbps
These act as relay nodes and you add them where needed to reach the End Device nodes.
One of these is necessary at least for initial configuration
Each devices has a unique 64 bit address
Routers may be added to gain distance or to get around blockages
Full-Function (FFD) or Restricted Function (RFD) End Devices
ZigBee Coordinator (FFD)
ZigBee Router (FFD)
ZigBee End Device (RFD or FFD) Very low power usage (battery)
Mesh Link (router to router)
Star Link (end node to router)

Figure 10.4 – The ZigBee wireless mesh architecture

Wireless Ethernet– Instruments (and other devices) that support wireless Ethernet (WiFi) can be connected into a larger, facilitywide, WLAN by the use of wireless repeaters and access points. This approach makes it possible to have WiFi service over a larger area without having to run cables and position Ethernet switches to create the network infrastructure. Figure 10.5 shows a very small WLAN comprised of three repeaters, one of which acts as a bridge onto a wired

Ethernet LAN. The two repeaters offer WiFi connectivity to local clients, which could be laptop PCs as well as instruments, sub-systems, and smart devices. Wireless Ethernet is not a low-power technology and so only powered (non-battery operated) instruments and devices, or devices only occasionally used, would be candidates for this approach. As was discussed in Section 6 wireless Ethernet needs to be made cyber secure via cryptographic methods such as applying the WPA-PSK or WPA-Enterprise standards to such a network.

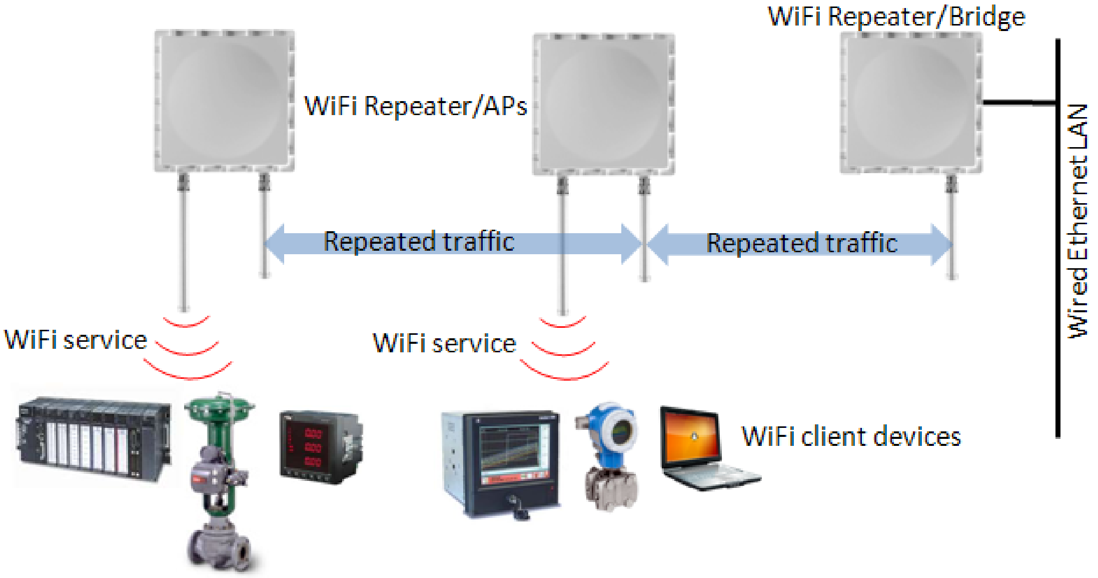


Figure 10.5 – Wireless Ethernet repeaters and access points

Advanced instrument capabilities– Many of the current array of smart instruments and control elements support a wide range of user-configurable calculation, logic, and control functionality and the ability to directly interact with other instruments (peer-to-peer communications) on the same LAN segment. This means that autonomous control, calculations, and even safety interlock functions can be configured in such devices. For example, a smart pressure transmitter could both measure pressure and also run a PID calculation (whose setpoint is adjusted with digital messages sent from an operator HMI also on the LAN segment). The pressure transmitter would then send the resulting valve position change (± change of % open) to the smart flow control valve via the instrument

LAN as a digital message. Figure 10.6 shows this concept being applied to a reactor water cooling loop.

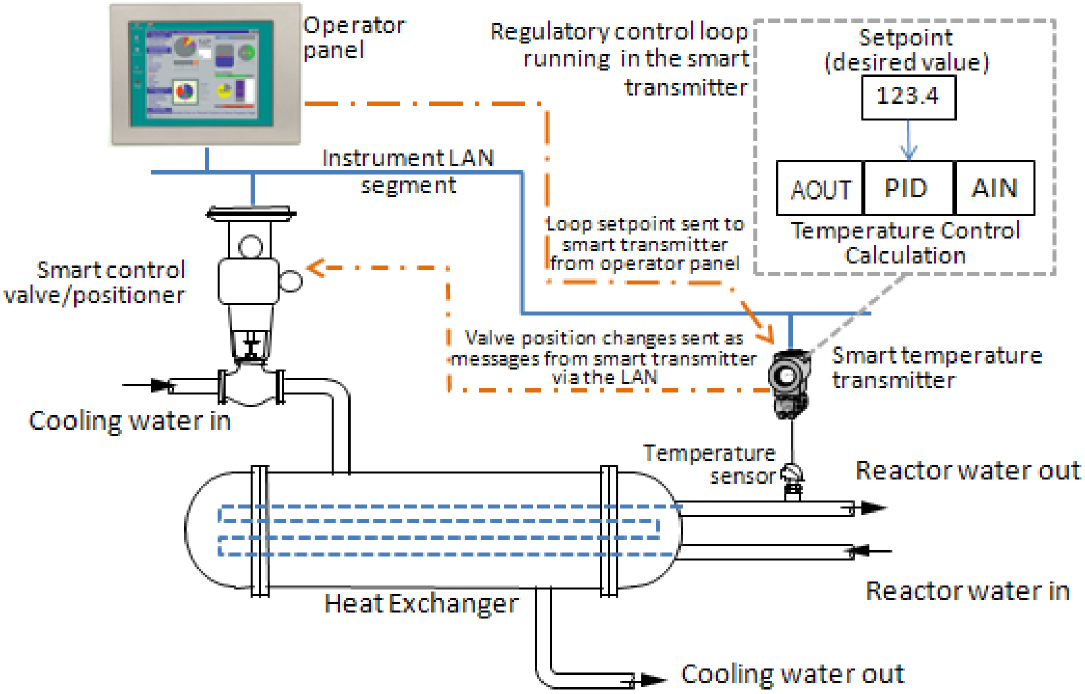

Operator panel
Regulatory control loop running in the smart transmitter
Setpoint (desired value)
123.4
AOUT
PID
AIN
Temperature Control Calculation
Instrument LAN segment
Loop setpoint sent to smart transmitter from operator panel
Smart control valve/positioner
Valve position changes sent as messages from smart transmitter via the LAN
Smart temperature transmitter
Cooling water in
Temperature sensor
Reactor water out
Reactor water in
Heat Exchanger
Cooling water out

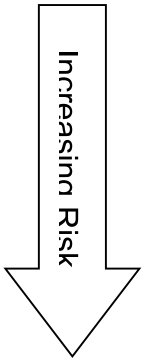
Figure 10.6 – Autonomous regulatory control using smart instruments

Using smart instruments in this manner potentially eliminates a lot of extra wiring and reduces the number of devices required (e.g., a separate PID controller was not required for the control loop in the example above). It also reduces the problem of maintaining instrument calibration and accuracy since the inter-instrument communication is done using digital messages rather than analog signals. From a cyber security perspective, the primary concern about using smart instruments in this manner is the unauthorized (and undetected) modification of the control logic and calculations running in those devices. A second concern is having someone make an unauthorized connection to such a LAN and issuing commands and parameter changes to the devices. Both of those threats require physical access to the instrument LAN or to the specific instruments. They also require the use of commercially available configuration tools, which could be easily obtained by the adversary. As was mentioned earlier in this section, there are a list of suggested actions that should be taken to physically secure such smart devices, their configuration tools, and their physical LAN. Configuration management and verification is also an important factor in the safe and secure use of smart instruments. Unlike with traditional analog instruments in which functional changes involved physically adding more modules and changing interconnecting wiring, with smart instruments alterations of control functions are not visible and obvious. Thus procedures are needed to review the active configuration settings on smart instruments and digital devices performing reactor control and safety functions, to verify that they are as expected and approved.

EP#71 – An effective cyber security practice is to confirm and validate that the configuration and settings of CDAs, digital devices and instruments are correct as part of reactor pre-operational checks.

Section 11: Upgrades, Replacements and Retrofits

Most NPR facilities currently have a reactor control system that uses a combination of legacy/obsolete, conventional analog control panel instruments. Most employ legacy computer hardware and software for supervisory control of their more advanced reactor power manipulations (e.g., pulsing the reactor or taking it to, and holding it at, a specified power level). At some facilities, there has already been an effort to make some digital upgrades, such as with digital trend recorders and digital panel displays. Some facilities have even attempted to make limited use of PLCs (programmable logic controllers) for data acquisition and supervisory control purposes or in non-safety applications (e.g., sample movement and timing). The application of digital technology can span a range of functionality with increasing levels being accompanied with increasing needs to address cyber security. The following list provides examples of possible digital technology applications ranging from very simple (digital indicators) and low-risk to more complex and higher-risk (digital safety shut-down):



- Digital indicators and displays
- Measurements and data acquisition
- Ancillary functions (e.g., Rabbit [sample exposure] control)
- Supervisory (manual) control of reactor via HMI
- Automatic (closed-loop) control of reactor variables
- Personnel & process safety interlocks
- Reactor (semi)automated operation
- Reactor safety shutdown/SCRAM

Like-kind replacements- Many licensees have already had to take steps to replace obsolete I&C technology, such as paper-based strip chart recorders and analog panel meters, with digital equivalents, if for no other reason than the lack of available spare parts (or paper in the case of the recorders). In general this practice does not pose an unacceptable cyber risk even though the replacement devices probably have many additional capabilities not present in the obsolete devices they replace. This is partially because licensees are generally <u>not making use of those additional capabilities</u> and partially because many of these devices are highly immune to cyber attack because of their hardware/memory design. In Table 2.1, two examples of like-kind device replacements were illustrated. The primary point being that the new digital devices had many additional (optional) functional capabilities, a major one being network connectivity. But what is also important is that many digital devices allow their basic functionality to be altered, possibly drastically, via manipulation of their configuration settings. This is not something that was normally possible with the obsolete analog devices; they were mostly single-purpose in their design unlike digital replacements that support a range of user-selectable (via configuration settings) functionality.

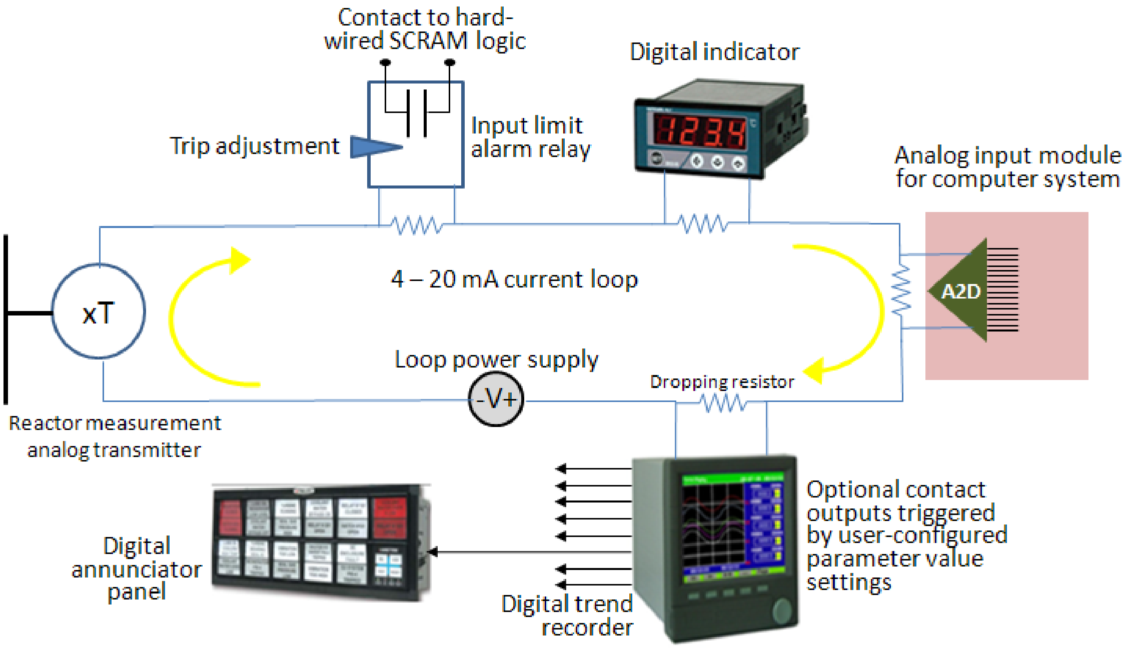

Contact to hard-wired SCRAM logic
Digital indicator
Trip adjustment
Input limit alarm relay
1234
Analog input module for computer system
A2D
xT
4 – 20 mA current loop
Loop power supply
-V+
Dropping resistor
Reactor measurement analog transmitter
Digital annunciator panel
Digital trend recorder
Optional contact outputs triggered by user-configured parameter value settings

Figure 11.1 – Digital I&C devices integrated into ‘analog’ circuits

Simple digital I&C devices can usually be placed into the same circuits as the analog devices they replace with no functional impact. Figure 11.1 shows a single analog measurement loop where digital devices (a digital trend recorder and digital indicator) have replaced the obsolete, legacy analog devices.

Their use in this manner would likely have no discernible impact on the safety or reliability of the reactor operation or on the ability to initiate a reactor SCRAM, but they would still need to be fully evaluated in accordance with 10 CFR 50.59. Similarly, the fact that the measurement is also being read by a computer program using an analog input module of some type, in the same loop, likely has no adverse impact on reactor safety or operation. In this type of configuration, the reactor operator has diverse means for observing the measured variable: via the digital meter, via the trend recorder, and via the computer system (if it is designed to provide a display of that information).

In the above example, the digital trend recorder is shown as have programmable contact outputs that are configurable to close/trip based on the associated measured value crossing a user-set value-limit. In principle, that capability could eliminate the need for a separate analog limit switch (wired as a SCRAM signal) in the loop. But the functioning of the chart recorder depends on its programming performing as designed/intended and on user-adjustable configuration settings being set correctly. This makes it theoretically less reliable and less deterministic than a simple hard-wired input limit alarm relay that only requires a given current flow through the loop to activate.

EP#72 – An effective cyber security practice is to not depend on software-based devices as the primary or sole means for initiating a reactor safety function or critical reactor operational/monitoring function. Analog/hard-wired circuitry is always preferable for reactor safety functions.

If the contact output(s) of the trend recorder were merely used to trigger a visual annunciator panel window (as indicated in Figure 11.1), and the analog input limit relay was still used for the reactor SCRAM function, this again would have no adverse impact on reactor safety, but it might provide a useful additional indication for the reactor operator.

Limited-functionality digital devices- Many digital devices used for I&C and physical security purposes are designed for stand-alone operation and some can operate in either a stand-alone or integrated (networked with other devices) mode. Many such devices have their program code burned into ROM (read-only memory) or stored in some other form of non-volatile memory (memory that retains its contents with power removed) so that they can immediately begin operation when powered-up. These devices usually do not have file systems, any form of multi-user/multi-tasking operating system and do not support the installation or addition of third-party applications. If used in a stand-alone manner (or are restricted to an isolated LAN), this makes them highly resistant to conventional forms of cyber attack and to most malware and staging a cyber attack would require gaining physical access to the device. This is again why having adequate physical security is an essential aspect for maintaining adequate cyber security. Figure 11.2 shows some examples of limited-functionality digital I&C and security devices that are highly immune to cyber compromise and conventional malware (malware not specifically designed and engineered to attack the particular CDA) when used in an isolated/stand-alone manner.

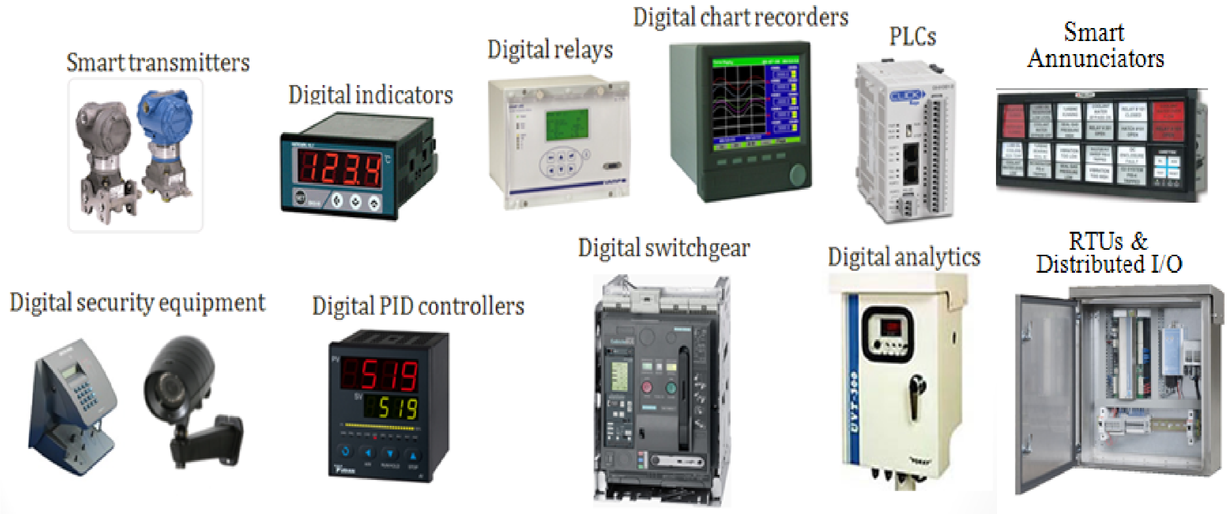
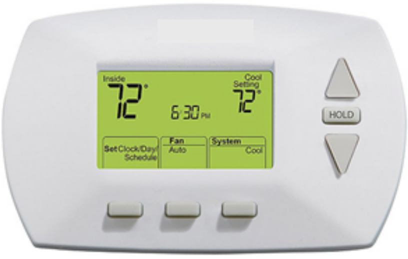


Figure 11.2 – Examples of limited-functionality CDAs

Of course not all digital devices will fall into this category. Any device that has, at its heart, some form of general purpose computer and commercial operating system (e.g., a Linux® or Windows© variant) will not have such immunity and would require additional technical measures to adequately protect it from cyber attack.

Configuration and operational settings – Just because a CDA is immune to most cyber attacks and malware does not mean that the device cannot be manipulated and its functionality significantly altered or disabled. Most digital devices have one or more operational settings that are used to adjust their actions. Many digital devices also have configuration settings that can significantly alter their basic functionality. Figure 11.3 illustrates the difference between **operational** and **configuration** settings using a digital thermostat as an example. Manipulation (malicious or unintentional/accidental) of operational settings could have a significant impact on how well a CDA performs its functions. But manipulation of configuration settings can totally alter the basic functionality of a CDA. In most cases, configuration settings are established when a device is put into service and generally never altered again. Adjusting configuration settings usually requires special training (and possibly special tools) specific to the respective CDA and should only be performed by personnel with appropriate knowledge and authorization.

Switching from heating to cooling (or the reverse) is a **configuration change** as it alters the basic function of the HVAC system



Adjusting the desired temperature over the supported range is an **operational parameter change** that has built-in limits (you can't dial in +1500 or -300 degrees.)

Figure 11.3 – The difference between configuration and operational settings

To use a more relevant example, one very common digital instrument is a microprocessor based single loop PID controller. These devices usually accept an analog input for the controlled process variable (e.g., pressure, temperature, flow), produce an analog output for adjusting the manipulated control element (e.g., a valve) and may optionally accept a second analog input as a remote setpoint value (see Figure 11.4). These devices usually offer a range of PID algorithm alternatives including error-squared, non-linear, reverse-acting, and ratio+bias (rather than PID). The desired function is generally set up as part of device configuration (as are things like tuning constants and bias values) and then usually never altered unless process changes are made. Often access to configuration settings requires knowing a password. During normal operation, it may only (at most) be necessary to adjust the setpoint for current operating conditions. Such operational changes normally do not require a password (which is the same as with an analog PID controller). Since altering configuration settings could radically alter the operation of the digital controller the ability to do so is a cyber security concern as it may require connecting a laptop PC to the controller. These controllers, as with many smart instruments, cannot be infected with malware as they have all their program code in ROM. But an infected laptop PC could maliciously alter configuration settings.

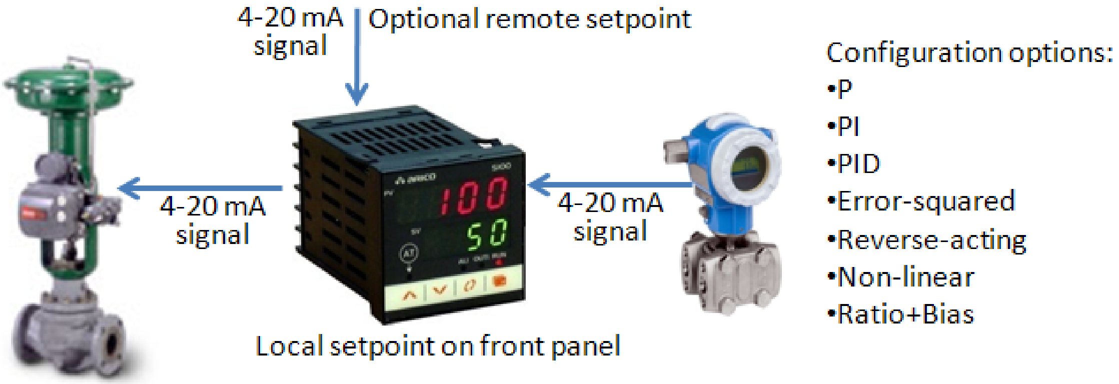


Figure 11.4 – A digital PID controller with a password-protected configuration

EP#73 – An effective cyber security practice is to restrict access to configuration settings on all CDAs using either physical measures (e.g., a locked cabinet) or logical measures (e.g., implement a password on the CDA) and to strictly limit the number of personnel who are authorized to make configuration changes. If a portable digital device (especially a laptop PC) is used to make configuration changes to CDAs then an additional effective practice is to limit and control access to the portable digital device and to vendor-supplied configuration software.

Reactor protection/SCRAM - Today the ability to automatically or manually initiate a reactor SCRAM is supported via hard-wired Boolean logic which essentially kills power to the electromagnets that couple the control rods to their positioners, causing the control rods to drop fully into the core. Any number of monitored conditions and manual triggers may be included in the circuit that kills power to the rod electromagnets. A set of contacts wired in series is logically an "OR" condition as any of them can cut the circuit and turn off the power (controlled by a relay indicated as SR1 in Figure 11.5). Of course loss of facility power or of the rod electromagnet power supply will also trigger a control rod drop. This fail-safe design is described in very general terms by Figure 11.5. All of the licensees surveyed by the staff currently use actual hard-wired relay logic to implement this fail-safe functionality.

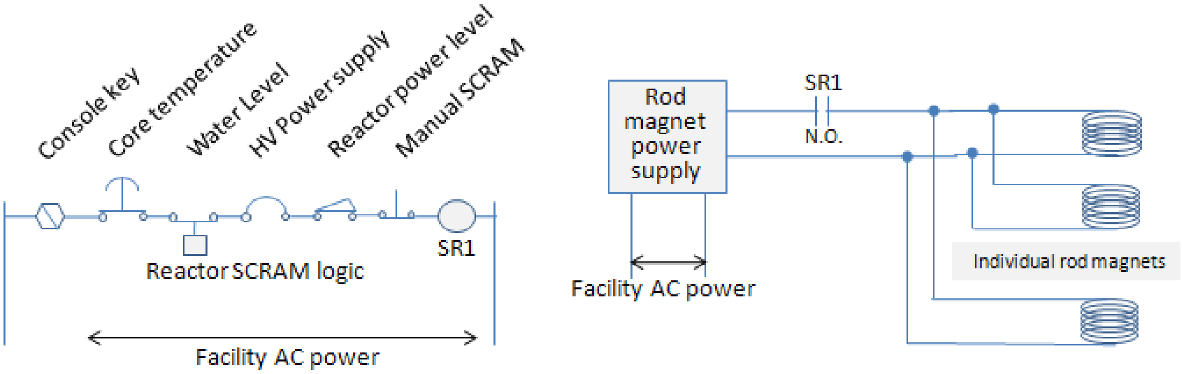


Figure 11.5 – Simplified reactor fail-safe SCRAM design concept

At some of the licensee facilities, the reactor safety functions have been augmented to include interlocks and derived SCRAM signals that are in addition to the parameter triggers required by the technical specifications ("tech specs") for the reactor. These may just be additional manual pushbutton signals for initiating a SCRAM or actual computed variables whose value can cause a computer program to toggle a contact output that is also wired into the SCRAM hard-wired logic. A highly simplified conceptual diagram of this approach is shown in Figure 11.6. In this design there are software-derived variables whose values are periodically updated and then compared to user defined limits. Crossing such a limit can then cause the software to change the state of computer-driven contact outputs which are wired into the SCRAM circuit. This design should not degrade or interfere with the effectiveness of the reactor safety system, but such changes would still have to be fully evaluated under 10 CFR 50.59. Those additional contact outputs are wired in series ("OR'ed") with the mandatory SCRAM signals in the fail-safe design and merely provide additional conditions under which an automatic reactor shutdown will be initiated.

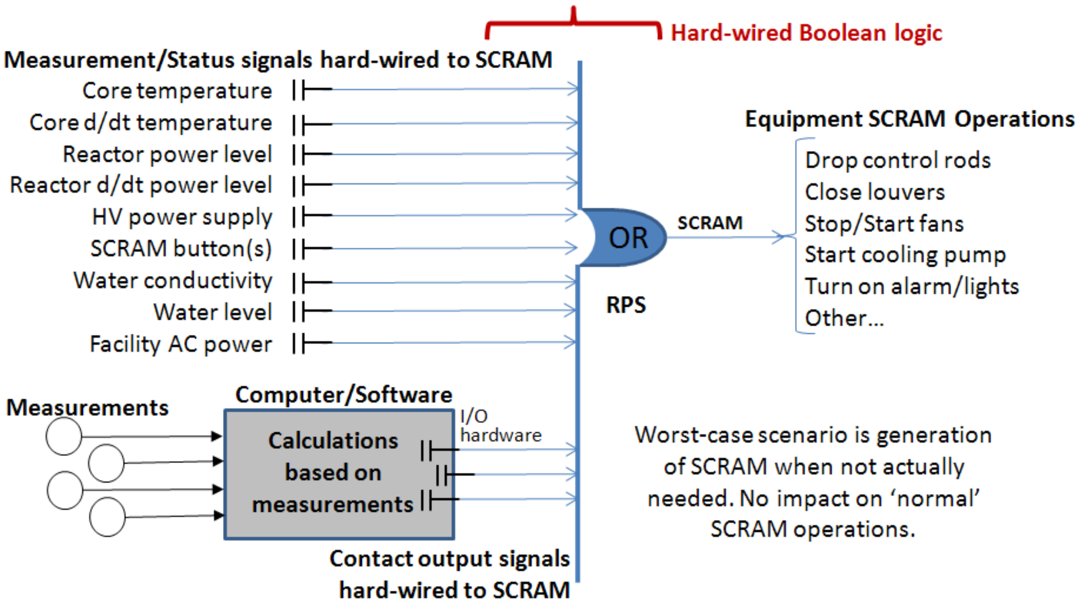


Figure 11.6 – Adding computed trip signals to the reactor SCRAM logic

Unnecessary SCRAMs might be triggered if the computer program contained logic errors (or was maliciously altered), but the computer would/could not interfere with mandatory (techspecs based) SCRAM operations.

EP#74 – An effective cyber security practice is to ensure that the malfunction or mis-operation (regardless of reason) of a CDA or digital system cannot interfere with or block the hard-wired reactor safety shutdown functions.

In the future, licensees may need to abandon the electromechanical relay design of the reactor safety system and replace it with modern digital technology. But this has to be done in a manner that is reliable and provides adequate safety. One approach that might be considered is to use PLCs to perform the same SCRAM logic as is implemented with electromechanical relays today. However, because PLCs (although proven to be very reliable in many other industries) are microprocessor based and depend on correct logic configuration, there is always a possibility of a hardware and/or software failure.

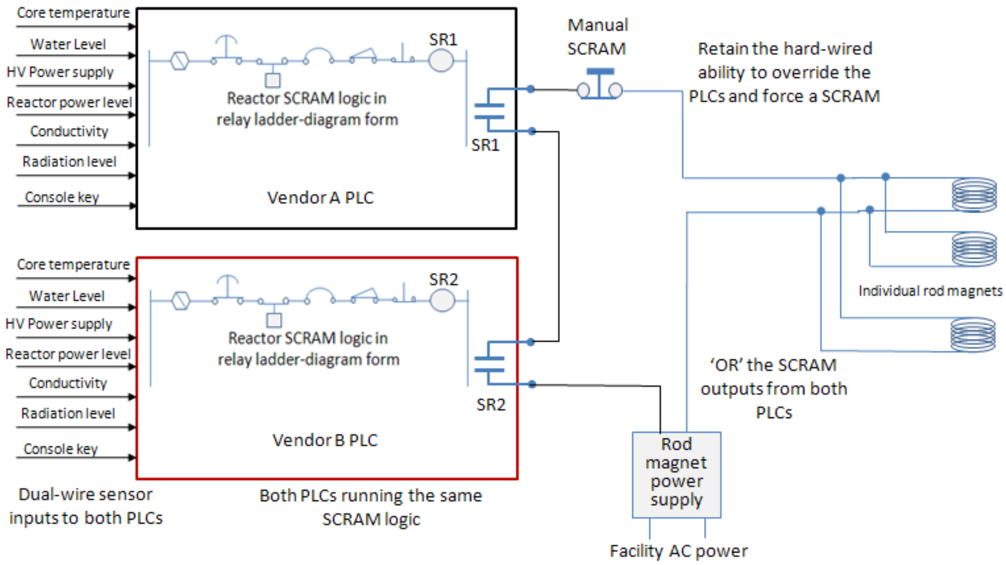


Figure 11.7 – Redundant PLCs used for a reactor safety system

When evaluating the use of a PLC-based system, consideration should be given towards using diverse, redundant PLCs, with hard-wired, manual SCRAM push-buttons wired in a fail-safe, series manner as one way to provide additional reliability in the design. Any such approach would still need to be fully evaluated under 10 CFR 50.59. Figure 11.7 provides a block diagram of a conceptual PLC reactor safety system design that incorporates redundant PLCs as well as a manual override capability.

EP#75 – An effective cyber security practice is that such a system should be isolated and physically secured and that maintenance, administration and configuration access would be monitored and strictly controlled through a combination of physical measures (e.g., locked, alarmed enclosures) and integral protective measures (e.g., keylock, passwords)

Section 11: Upgrades, Replacements and Retrofits

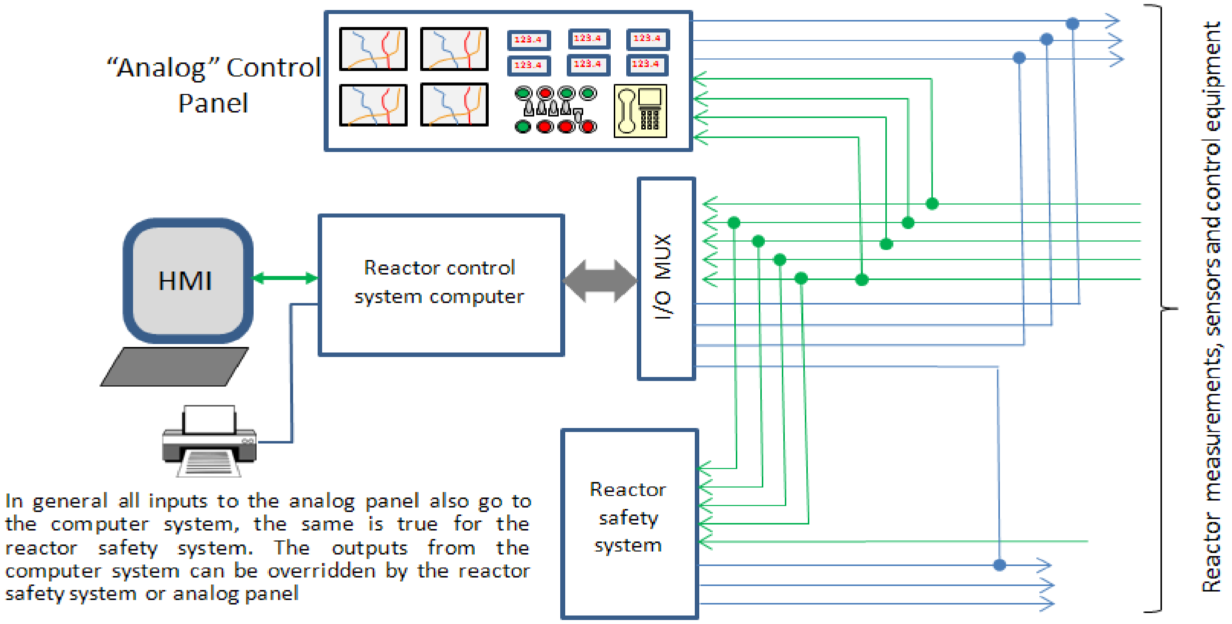
EP#76 – An effective cyber security practice where PLCs or other types of digital devices employ a physical key to enable logic modifications (to be put into program mode) the key should be kept secure and anti-tamper measures (e.g., tamper seals) should be used to detect unauthorized access to the PLC equipment.

Changing computer platforms– Many of the NPRs have legacy computer hardware and operating systems and are running proprietary application software developed by General Atomics to support reactor operations. To a degree, this has made those systems less vulnerable to cyber attack since they lack TCP/IP network support, are isolated, don't have USB ports, don't have all of the bells and whistles that come with modern multi-user/multi-tasking operating systems, et cetera. But it is inevitable that these hardware and software platforms will eventually be replaced with new platforms that may be far more susceptible to existing forms of cyber attack and malware. Because of this, it will be important, as part of any computer upgrade project, to address and include cyber security as a required element of any such project. There is no single thing that can be done (aside from never turning it on) to make a modern computer safe from cyber attack. And there are factors, such as having external network connectivity, that add to the difficulty and to their vulnerability. In general terms, the things that should be done to minimize a computer system's vulnerability to cyber attack amount to a process called hardening. Hardening is somewhat operating system specific and not something that will be addressed in this document. There are references available that describe how to harden various operating systems including NIST SP 800-70, *Security Configuration Checklists Program for IT Products*. There are also third-party software products grouped under the general heading of Host-based Intrusion Detection Systems (HIDS) that can be added to most modern operating systems and that will detect (and potentially block) attempts to make malicious alterations to system software and settings.

EP#77 – An effective cyber security practice for maintaining the integrity of modern multi-tasking operating systems and associated applications is to employ some form of HIDS package that blocks unauthorized manipulation of the operating system settings and security functions and prevents unauthorized software (e.g., malware) from being allowed to execute. This is also called "white-listing" as it involves defining what software is authorized ('white') to run while everything else is blocked from running and treated as untrusted/unauthorized.

NIST has published SP 800-94 "Guide to Intrusion Detection and Prevention Systems," which offers extensive guidance on the various types of commercially-available HIDS products. It has already been mentioned that CDA isolation is preferable if possible although that brings in new problems. For example one aspect of hardening is keeping security-related patches up-to-date. This is often easily accomplished if a system/CDA has internet access, but is made more complicated if a system is isolated.

Digital Supervisory Systems – The existing reactor control systems at most of the NPRs surveyed consisted of both manual/analog indicators and controls and some level of computer-based data acquisition and supervisory control via their legacy computer-based reactor control system. All of the designs surveyed included a level of cross-wiring of inputs and outputs among the analog panel, the control system computer, and the reactor safety system (as shown in Figure 11.8).


"Analog" Control Panel
123.4
HMI
Reactor control system computer
I/O MUX
Reactor safety system
Reactor measurements, sensors and control equipment

In general all inputs to the analog panel also go to the computer system, the same is true for the reactor safety system. The outputs from the computer system can be overridden by the reactor safety system or analog panel

Figure 11.8 – Highly simplified block diagram of existing NPR reactor systems

For inputs, this mainly means that the 4-20 mA analog input signals pass through all three sub-systems in a manner similar to that shown in Figure 11.1 and can be used by all three simultaneously. For outputs this is a bit more complex. Contact outputs from two different systems can easily be "OR'ed" or "AND'ed" by wiring them in series or in parallel across any combination of the three sub-systems as shown in Figure 11.9.

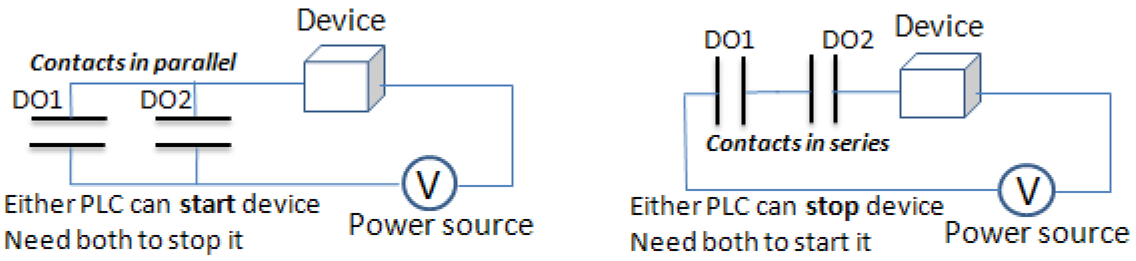


Figure 11.9 – Wiring contact outputs in series or parallel

Analog outputs (if used) can be wired to allow them to be controlled by either the computer system or the analog control panel with a manually-controlled selection made via the analog control panel. The computer system supports both data acquisition and supervisory (manual and automatic) control of outputs. Supervisory control means the computer software controls the analog/contact outputs but will take its direction from either an operator via the HMI (manual mode) or from application software running on the computer (automatic mode). Reactor equipment control signals generated by the computer system currently are dual-wired with the analog control panel so that the operator can override them if needed. In a future control system digital replacement, a typical approach might be to use a PC/PLC combination to replace the manual (analog) control panel and the legacy computer system. Figure 11.10 shows the sorts of components that could be used to construct a replacement system. Of course, reliability considerations might dictate having at least two operator consoles and having a redundant PLC design. The reactor safety system would be separate from this control system.

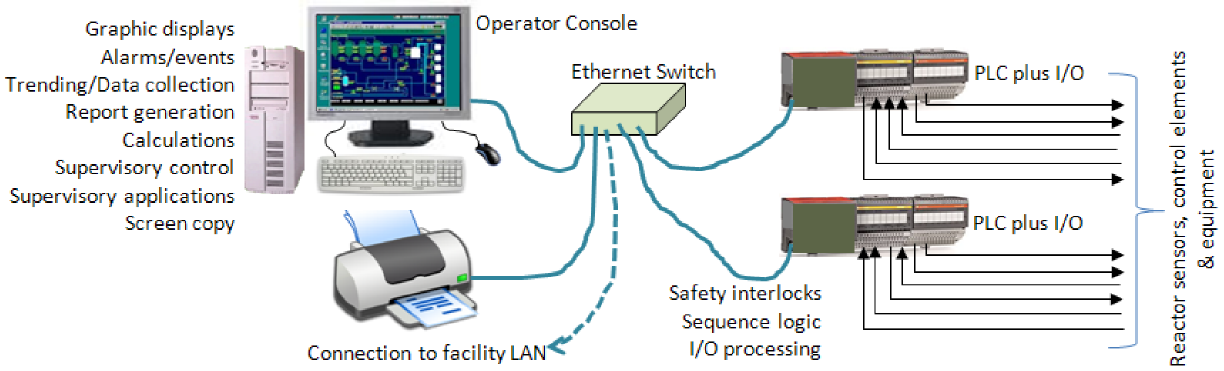


Figure 11.10 – Potential future digital reactor control system architecture

From a cyber security perspective, such a system is very similar to the ones attacked and subverted by the now-famous Stuxnet malware suite.

EP#78 – An effective cyber security practice would be to take specific measures to ensure that adequate cyber security was maintained. The types of measures required (e.g., hardening, HIDS, white-listing, etc.) were already discussed previously in this section. Proper use of portable media (see Section 9) would also be essential for adequate cyber security (recall that Stuxnet was introduced via portable media).

Although the failure or malicious manipulation of a digital reactor control system might not result in the release of any radioactive material or a radiological sabotage event, it is still essential that a separate reactor safety system be used (even if digital itself) to ensure that a SCRAM can always be initiated if necessary.

EP#79 – An effective cyber security practice and essential design concept, in any future digital upgrade of the reactor control system, is that a malfunction of the reactor control system (whether due to hardware or software) must not be able to block execution of the reactor SCRAM function.

Ancillary/non-critical systems – Several of the NPR licensees have indicated an interest in using PLC/PC technologies for non-critical (non-reactor control/safety) functions such as pneumatic system (rabbit) control and timing and sample exposure management. There are three obvious approaches/options that could be taken to implement such capabilities:

1. Use a separate, isolated set of equipment (PC/PLC) for this purpose
2. Use a separate, but LAN-connected (with the reactor systems), set of equipment (PC/PLC) for this purpose
3. Add this incremental functionality (additional I/O and additional PC software) as part of a reactor control system digital upgrade

With option one above, the primary cyber concern would be the possibility of malware being spread from this system to reactor control/safety systems via portable media. If suitable portable media usage procedures and policies are implemented (see Section 9) and the PCs involved are hardened (refer to the "changing computer platforms" paragraph within this section), then this concern is reduced to an acceptable level.

With option two above, the primary cyber concern is the possibility of malware being passed from this system via the common LAN, as well as via shared portable media. If the reactor control system is on a separate LAN segment, isolated from this system by an internal firewall (refer to Section 6), media usage is addressed (per Section 9) and the PCs involved are hardened (refer to earlier in this section), then this concern is reduced to an acceptable level.

With option three above, the primary cyber concern would be that incorporating these additional ancillary functions into the reactor control system could somehow interfere with the reactor operation functions or with the operator's ability to interact with the HMI and monitor/control the reactor. Although modern PLCs and PCs have vastly greater processing, memory, storage, and communications resources than the current GA reactor control systems, it will be very difficult, in advance, to provide a deterministic analysis that proves that such an interaction could not occur. Because of that fact, this last approach might not be recommended.

EP#80 – An effective cyber security practice is to use separate systems and equipment, potentially on a separate LAN segment, for ancillary NPR functions rather than risking the possibility of those additional functions interacting with or interfering with the essential reactor safety and operational functions were they integrated into the systems that perform those critical functions.

Procurement practices and testing requirements – One of the potential attack pathways mentioned in Section 4 was the supply chain. This is a general term that applies to all of the various ways in which a CDA could be cyber compromised, either during its fabrication or once placed into operation. Supply chain issues range from having products with undocumented and unauthorized functionality (e.g., a secret vendor account [a.k.a. a backdoor]) or that contain a time-bomb (program code set to execute based on pre-defined conditions/time) to having vendor personnel who are paid/coerced into making improper setting changes (e.g., disabling alarming functions) during a maintenance or upgrade activity. Today, when computer systems/digital devices are purchased and serviced, or custom software is developed, it is essential that the procurement process include and specify appropriate cyber security testing and validation requirements.

Software assurance – The Department of Homeland Security (DHS) has developed a set of guidelines and recommended practices regarding software assurance, which are aimed at ensuring that software does not contain any unauthorized/hidden functionality or well-known coding/design weaknesses or exploitable cyber vulnerabilities. Although these guidelines are primarily aimed at custom software development efforts (including those subcontracted), it is also useful to find out if the vendor of COTS software has an internal software assurance program.

A basic requirement of software assurance and a commonly used method of verifying that purchased products and systems meet cyber security objectives is to perform (or require the vendor to perform) both functional and cyber security testing as part of a procurement. Functional testing proves that the product/software/system performs all of the specified functions, whereas cyber security testing attempts to verify that the software/system/device does not contain any known, exploitable cyber vulnerabilities.

EP#81 – An effective cyber security practice is to always include cyber security testing (or proof of such testing) as a requirement in procurements. For contracted software development this should include having the developer follow secure coding practices and perform and/or document:

- *Peer code reviews*
- *Static code analysis*
- *Vulnerability scanning*
- *Known vulnerability testing*
- *Secure language/library selection*

There are also independent certification standards such as ISASecure® (IEC 62443 compliance certification) that establish a set of cyber security specifications and processes for the design, testing, and certification of critical control systems and instrumentation products. A product that carries an ISASecure certification is supposed to have been designed and tested to be at least highly resistant to known cyber attack methods and cyber tampering.

Another recommendation for addressing supply chain issues is to establish a trusted vendor program. In many cost-conscious environments, it is tempting to purchase products from the vendor offering the lowest available price. In some cases, this can lead to the purchase of a device with counterfeit parts or software. This can lead not only to a potential cyber security risk but also reliability issues.

Potential equipment and software vendors should be reviewed for trustworthiness using criteria appropriate to the risk profile of the components involved. The following are some potential considerations to investigate:

- Are they the original product manufacturer?
- Are they an approved reseller or partner?
- Do they have a positive reputation within the community?
- Have they been involved in or associated with any cyber incidents, legal actions, sanctions?
- What is their point-of-origin?

Performing the necessary due diligence on a potential vendor can provide confidence in the provenance of the devices or software. Vendors who meet the criteria established by the organization are then placed on an approved vendors list, and procurement activities can be limited to these vendors.

A trusted vendor program focuses your supplier pool by prequalifying suppliers. Higher risk suppliers can be eliminated from the procurement chain. However, it is important to understand that there is a tradeoff to focusing the supply base in the form of reduced competition and, as a result, potentially higher prices.

Section 11: Upgrades, Replacements and Retrofits

EP#82 – An effective cyber security practice is to develop a trusted vendor program restricting procurement of devices and software only from pre-approved vendors or from vendors who meet the appropriate qualifications and requirements prior to purchase.

Section 12: Future Trends in Digital Technology

Although in the near term many NPR licensees may be forced to adopt digital technologies piecemeal due to obsolescence issues and the inability to maintain, repair, or replace their analog instrumentation. In the longer term, licensees may wish to make a greater use of then-current digital technologies. This report makes no attempt to predict what those technologies might be, but it can be presumed that they would be advancements on many current digital (computer-based) technologies that are in common use today in other industrial segments. Looking at just the reactor systems possible digital technologies include the following:

1. Local Area Networking, both wired and wireless
2. “Smart” instrumentation and instrumentation LANs
3. Digital signal processing technologies
4. High-speed data capture and storage
5. Relational database information storage
6. PLC and PAC microprocessor controllers
7. Wireless devices such as tablets and cell phones
8. User-configurable operational displays
9. Commercial SCADA/HMI software
10. Web-based informational/operational displays
11. Smart alarming/alarm management
12. Equipment condition monitoring
13. Biometric authentication
14. Automated diagnostics
15. Autonomous regulatory control
16. Interaction/data exchange with other site systems (e.g., HVAC)
17. Mathematical models and model-based control
18. Cloud computing and information storage

Section 12: Future Trends in Digital Technology

EP#83 – In general terms the most important consideration and effective practice, from a cyber security perspective, when applying ANY digital/computer technology is to ensure that a malfunction (accidental or malicious) of that technology (all or part) cannot prevent/block the reactor safety system from performing a SCRAM. The second most important consideration is to ensure that reactor operators have a diverse means of seeing the current values of essential reactor operating parameters so that a malfunction (accidental or malicious) in any one device/subsystem cannot 'blind' the reactor operator to the true value of any of those reactor operating/safety parameters.

As such the licensee must document and demonstrate to the NRC via the 50.59 or license amendment regulatory process that such changes will maintain the safety margins and the methods approved by the NRC in establishing those margins.

Since theft and diversion of nuclear materials is the major threat facing NPRs, the evolution of digital systems and equipment augmenting and supporting physical security must also be considered. Most of these systems are currently fully digital but possible digital technology advancements in those areas could include the following:

1. New/expanded biometric recognition factors
2. Facial recognition software
3. Automated video analysis
4. Enhanced chemical sensor technology
5. Automated threat analysis
6. Automated threat neutralization
7. Automated defensive measures
8. Smart card technologies
9. Fiber optic LAN technology
10. Fault-tolerant wireless communications
11. Wireless sensors
12. Wireless video surveillance

13. Advanced intrusion sensory technologies

The primary consideration in the adoption of any such technologies is to have a cyber security impact analysis performed to determine if there will be any security weaknesses or exploitable cyber vulnerabilities introduced because of their use or incorporation.

Section 13: NPR Functions that could be Digitalized

Although current NPR designs do not tend to use digital technologies to any great degree, except for their physical security implementations, the NRC recognizes that in the future this may change. There are a range of activities and functions associated with the NPRs themselves, and their facilities, that could potentially be partially or fully automated using digital technologies. Some of the activities proposed by licensees for future digital automation include the following:

Reactor cooling (heat exchanger)
Ventilation/scrubber control
Control rod positioning
Reactor SCRAM
Radiation monitoring
ESD/Safety monitoring and interlocks
Pool pH/conductivity monitoring and control
Basic reactor parameter monitoring
Sensor measurement validation
Operator action logging
Operator sequence prompting/checking
Event/alarm logging
Report generation
Reactor physics computations
Sample exposure/movement control
Reactor system self-test/pre-start test
Reactor diagnostics
Reactor power curve auto generation

Experiment data acquisition
Experiment sequencing/control
LINAC ancillary functions
Beam focusing
Beam timing
Beam safety interlocks

Section 14: Summary

The NRC recognizes that NPR facilities currently face a transition point – most are attempting to maintain their operations using non-digital and increasingly obsolete computer technologies with the spare parts needed to support them either no longer available or becoming scarce. To maintain their operations into the future, most NPR licensees will need to adopt commercially available digital instrumentation and control (DI&C) and computer-based automation technologies. Beyond merely maintaining their operations, many licensees have indicated that they could enhance their research activities and improve operational efficiency by the judicious application of available digital technologies.

The protection of the public and environment is the NRC's primary mission. The NRC recognizes that adoption of digital technologies without adequate assessment of the attendant cyber security risks could lead to concerns regarding safety, security, emergency preparedness, and material control. The purpose of this effective practices document is to provide RTR licensees with information about how to use digital I&C technologies and modern computer and networking technologies in a manner that provides adequate cyber security protections and mitigates the risks. These effective practices are applicable to the reactor safety and operational systems but are equally applicable to the physical security support systems used at the NPR facilities.

A basic guiding principle for any effort to adopt and integrate digital technologies into an NPR facility is that all such changes must be made in a manner that ensures that the mis-operation or failure of digital systems or devices, regardless of cause (including malicious actions), must not prevent or otherwise interfere with the safe shutdown of the reactor and must not blind the reactor operator to the true values of essential reactor operational parameters. These will be the basic criteria that must be met when proposing changes to the current NPR reactor operational design.

Glossary of terms

No.	Term/Acronym	Definition/Meaning
	4-20 mA	An analog signaling method using an electric current that is varied between 4 and 20 milliamperes in value as a means for representing a corresponding process measurement value range (e.g., 0 to 100 gpm.)
	ASCII	American Standard Code for Information Interchange. A 7-bit binary code used to represent all of the English language letters (both cases) as well as punctuation, numbers and various special character codes.
	Base64 Encoding	The presentation of a large binary number (e.g., 128 bits) in the form of a series of printable ASCII characters to make it more manageable. The binary number is broken into groups of 6 bits and each group, based on its value, corresponds to a printable ASCII character.
	BIOS	Basic Input/Output System – The (EP)ROM based bootstrap program that begins execution when power is applied to a computer and which normally runs a set of hardware checks and then loads the operating system into RAM memory from the specified bulk memory device (e.g., a hard drive) and starts it executing.
	DB-9 or DB-25	The mechanical and electrical specifications for a male/female connector and jack used for EIA/TIA-232 serial communication ports on digital devices and computers.
	Digital Asset	A device or system that incorporates one or more microprocessors/CPUs and associated stored program instructions that direct the functioning of the device or system.
	Encryption	The fully-reversible process of converting information into an incomprehensible form (and eventually back into its original form) through the use of a known conversion algorithm and a shared (secret) key.
	HART	Highway-Addressable Remote Transmitter; a communications protocol suite that is used to interrogate, configure and inter-operate among compatible process instruments via their twisted-pair analog signal wiring.
	Hardening	The process of eliminating or reducing the potentially exploitable vulnerabilities in a computer system/device to make it immune to as many known cyber attack methods and malware as is possible.

Glossary of terms

Hash	A fixed-length binary number generated by a hash algorithm through the processing of an arbitrarily-sized data set in a manner that creates a unique resulting value, usually displayed in Base64 encoding
HMI/MMI/HCI	Human-machine interface, Man-machine interface and Human-Computer Interface. All three refer to the equipment used to allow a digital system/device to interact with a human being. For a typical PC this would refer to the keyboard, mouse and video display.
I/O	Input/Output – referring to analog (e.g., variable voltage or current), contact and pulse signals used to interface a digital asset with process measurements and process equipment for the purpose of monitoring and controlling them.
ISO/OSI	International Standards Organization, Open system Interconnect. A seven-layer model for creating communications networks with interoperability across different vendor platforms.
Operating System	Also referred to as the O.S. - the basic program code that controls, allocates, protects and manages all of the resources of the computer/system in which it is executing including the CPU, main memory, peripheral devices and bulk memory.
Key	A large binary number (e.g., 128, 256, 1024 bits) used as a shared secret/password by various types of encryption software. A special type of mathematically-related pairs of keys are called a Public-Private key set and are used in many on-line cryptographic applications.
LAN	Local Area Network. A communication network with physically limited geographic coverage and a small to moderate number of intercommunicating devices. Ethernet is an example of an IT/Computer LAN. Fieldbus and Profibus are examples of an instrumentation LAN.
Port	This can refer to a physical/electrical interface used to make a connection between a computer and another device (e.g., a USB or Ethernet port) or it can refer to a TCP or UDP protocol numeric association used to provide message traffic delivery to and from the appropriate application programs running on their respective computer and communicating across an IP-based network.
RdBMS	Relational Database Management System. A set of software that supports the creation, editing, alteration and deletion of relational

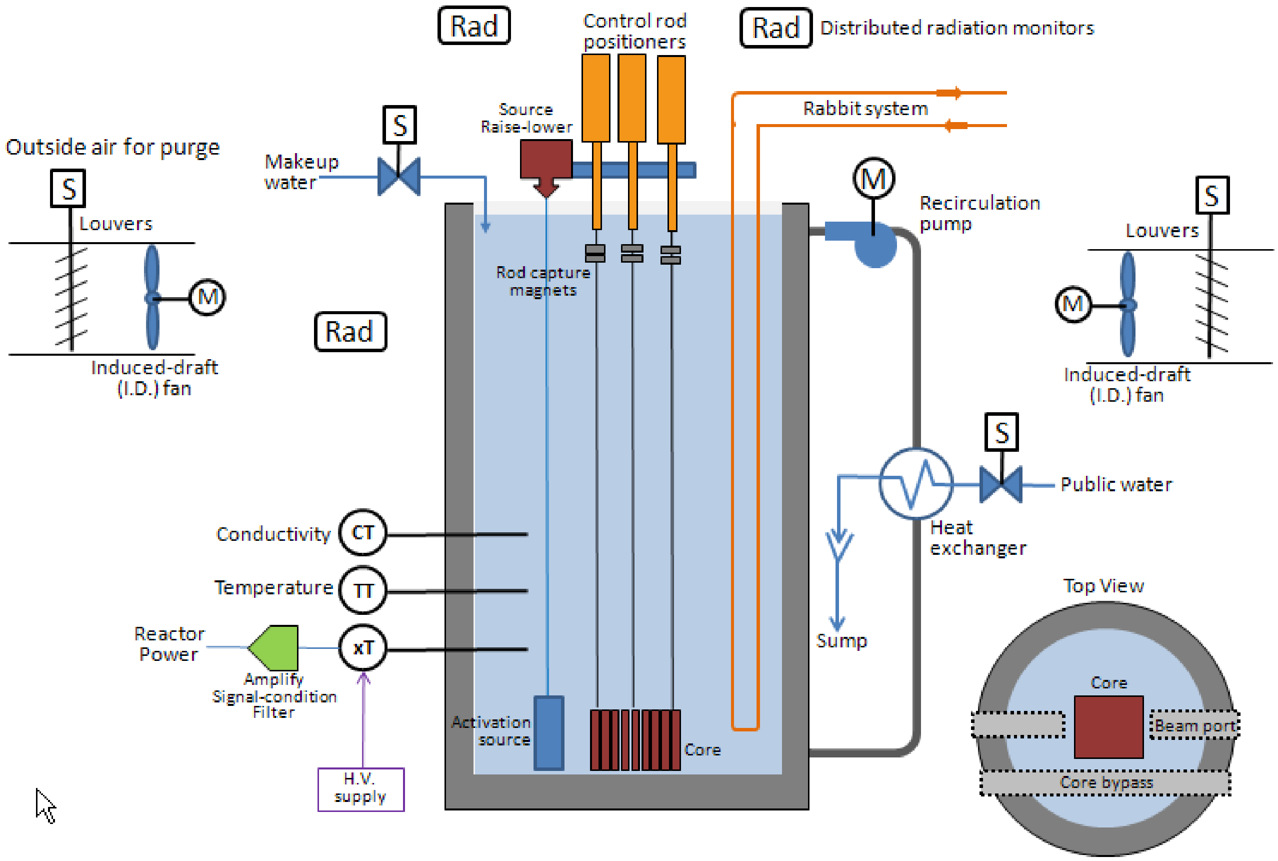
	databases and provides a user and application interface for interacting with and querying such databases.
Security control	Also called ‘controls’ – a measure, device, action or activity put in place to counter a potentially exploitable weakness or vulnerability. Security controls tend to fall into three main categories: physical, technical and administrative.
Smart devices	Devices that incorporate a microprocessor and stored program code. See Digital Asset.
WAN	Wide Area Network. A communication network with essentially unlimited geographic coverage and a potentially huge number of intercommunicating devices. The Internet is an example of a WAN.
WiFi	Wireless Fidelity, a certification that a wireless Ethernet device (such as an access point or router) is compliant with the applicable IEEE 802.11 standards and will interoperate with other certified devices. Often used as a general term to mean wireless Ethernet.
UTM	Unified Threat Management – a marketing term used to describe the latest evolution of advanced, next-generation firewall technology.

Appendix A – Revision log

Revision No.	Major	Significant	Minor	Approved By	Date	General Description of changes
A-1.0	x			W.T.Shaw	May 30, 2015	Initial release of the document

Appendix B – NPR reference model

The following diagram is intended to provide a generalized representation of a typical research and test reactor to assist in associating references made in this document to the various components of a research and test reactor.



Appendix C – Effective practices summary

No.	Effective practice summary	Section	Page
1	Provide adequate physical security measures to ensure that unauthorized personnel cannot gain access to critical digital assets and networks.	4	11
2	Provide backup power that can support continued operation for 25% longer than the worst-case time interval.	4	13
3	Physically secure CDAs using locks that are highly resistant to compromise, and employ a key management system.	4	14
4	Implement a multi-factor authentication scheme to augment RFID badges to decrease the likelihood of a stolen or cloned badge being successfully used to gain unauthorized access.	4	15
5	Use of badge carriers/covers that prevent surreptitious RFID cloning.	4	15
6	Minimize and protect the available cyber attack pathways that might be used by an adversary.	4	16
7	Eliminate or disable unnecessary communications pathways to CDAs; protect necessary communications pathways with security controls.	4	16
8	Use port-locks and other access prevention devices on unused communications ports.	4	17
9	Isolate systems that contain sensitive and classified information in electronic form and protect the data at-rest using either full disk encryption or folder encryption as well as a BIOS password.	4	18
10	Use a BIOS password to prevent a laptop from being booted by unauthorized personnel.	4	18
11	Enable either full-disk encryption or selected folder encryption of computers and laptop PCs that contain SGI, classified or sensitive information.	4	20
12	Add or enable tamper-detection functionality to CDAs and, where possible, tie that detection capability into the physical intrusion detection system as alarm inputs.	4	21
13	Use physical security measures such as metal conduits, metal junction boxes with anti-tamper screws, low-accessibility internal routing.	4	22

Appendix C – Effective practices summary

14	Always change CDA factory default passwords; create password and user account policy to define account assignment, password complexity, password lifetime, password change criteria, account disabling for PCs using commercial operating systems.	4	22
15	Create password and user account policy for specialized devices. Policy may allow for compensating physical controls for low-functionality devices.	4	23
16	Enable account locking on CDAs after a modest number of failed login attempts where supported.	4	24
17	Physically isolate CDAs (no communications connectivity) so that physical access (to the facility and CDA) is required to adjust, manipulate, configure or service the CDA.	4	25
18	Use integrated CDA password capabilities where possible and assign the strongest possible passwords to replace vendor/factory defaults passwords.	5	27
19	Secure each CDA using physical protection, anti-tampering measures, tamper detection, unique passwords, battery/data backups, disabling of remote access, logical isolation, security testing, change management.	5	28
20	Use protective devices that can inspect, detect and block malicious and unauthorized message traffic, including attempts to deliver malware, between the intermediate (university/corporate) network and the NPR facility.	6	32
21	Use firewalls that can identify the specific message types, and source/destination ports/addresses; use strong rulesets in an “unless allow, deny” configuration.	6	33
22	Update firewall and malware/attack detection rules and signatures on a monthly basis or when the vendor provides notification that an essential security update is available.	6	33
23	Use host-based firewall software on all office automation systems, PCs and laptops of the NPR facility.	6	33
24	Avoid the use of dual NICs and the simultaneous connection of any computer or “digital” device to both trusted and non-trusted networks.	6	34
25	Always disable all wireless interfaces of a laptop PC when connecting it to a wired LAN that contains CDAs, or if the laptop PC is itself a CDA.	6	35

Appendix C – Effective practices summary

26	Segment LANs using firewalls where isolation is not possible, group assets of similar importance/sensitivity into common segments, and place the most essential assets behind the greatest number of firewalls and the greatest number of message/traffic restrictions.	6	36
27	Avoid using KVM switches between trusted and untrusted networks. Using them to connect with multiple computers that are all on the same trusted network is acceptable.	6	37
28	Prevent accidental connection of critical systems and devices to the wrong network by employing a color-code scheme with Ethernet cables and network distribution wall plates.	6	37
29	Achieve LAN reliability by implementing separate replicated LANs with independent cabling, routing and switching. Devices may be connected to both LANs or may have a manual failover method.	6	38
30	Use physical barriers to protect ‘serial’ industrial protocol interfaces to digital (“smart”) devices such as metal conduit and junction boxes for the circuit wiring and using locked, alarmed (door switches wired into the physical intrusion detection system) enclosures.	6	40
31	Use dedicated communications wiring for ‘serial’ industrial protocol interfaces to digital (“smart”) devices and avoid ‘tunneling’ such communications through Ethernet-TCP/IP networks.	6	40
32	Protecting important and sensitive network traffic (video or otherwise) from tampering, unauthorized access and spoofing by creating a permanent site-to-site VPN.	6	42
33	Ensure that the security organization monitoring the NPR facility alarms and/or surveillance video stream itself has an effective cyber security program to prevent their systems (and the VPN connection to the NPR facility) from constituting a pathway for cyber attack.	6	43
34	For CDAs that cannot operate properly or effectively without a shared LAN connectivity, create and maintain a dedicated local isolated LAN to interconnect them including providing adequate physical security for the isolated LAN components, active elements (e.g., a switch) and cabling/media.	6	43

Appendix C – Effective practices summary

35	Isolate all network-connected CDAs associated with a given function (e.g., physical security, reactor control and protection, emergency response) on their own, individual isolated LAN segments.	6	44
36	Avoid the use of wireless communications for essential, critical and reactor-safety functions. Hard-wired connections should always be employed for those functions and applications.	6	45
37	Secure WLANs by implementing WPA2 cryptographic functions in all wireless routers and wireless clients using WPA-Enterprise mode; use a central server for wireless user authentication; generate individual session keys for each wireless client.	6	46
38	Disable all wireless capability on printers, scanners and other network-shared peripherals and to attach those devices to a wired LAN segment.	6	47
39	Disable all wireless communications capability on all computers and devices connected to a trusted network.	6	47
40	Require cell phones with hot-spot functionality to be turned off or kept out of any area where wireless-enabled CDAs are in use.	6	48
41	Employ a deterministic one-way device, such as a data diode when securely transferring information from CDAs and trusted networks to untrusted systems and networks.	6	50
42	Protect DMZ systems that provide reactor data to external users using: system hardening, white-listing, updates/patches, function/service restrictions and prohibiting other systems from being placed within the same DMZ.	6	51
43	Install a NIDS on the NPR facility LAN to: inspect all message traffic entering and exiting; identify malicious, suspicious, unauthorized and questionable messages; and provide a notification to appropriate NPR administrative personnel.	6	53
44	Develop and maintain a list of information about and applicable materials for each identified CDA within the NPR facility, such as: software inventory, manufacturer make/model/serial, patch level, location of install media, license keys, backups, special peripherals (keys or dongles), account list, admin list, master passwords.	7	56

Appendix C – Effective practices summary

45	Restrict the number of personnel granted administrative rights/accounts on each CDA and ensure that all admins have applicable training and experience in CDA administrative functions.	7	58
46	Disable CDA communication functions that are not required, utilize local CDA ‘console’ ports for administration where possible.	7	59
47	Use authenticated and encrypted remote access functionality such as SSH and HTTPS; assign each CDA a strong unique password.	7	59
48	Limiting and manage remote administrative access to CDAs to use mobile client VPNs with temporary (short-duration validity) digital certificates.	7	62
49	Develop procedures to ensure that any telephone modems and phone lines used for temporary remote access are disconnected and removed once the administrative activity is completed.	7	64
50	Use temporary accounts/password for remote administration/maintenance of CDAs, ensure necessary backups are made prior to remote maintenance, review and document remote maintenance activities prior to initiation. Employ HIDS on CDAs that are the target of remote administration. Employ system hardening, HIDS and antivirus on computers used for remote administration/maintenance.	7	65
51	Ensure that all NPR personnel receive a basic introduction to cyber security, ensure that personnel performing administrative functions and/or utilizing CDAs receive an additional level of cyber security training.	8	66
52	Ensure that all NPR personnel, and those working with digital systems and assets at the NPR facility are aware of existing university/organizational IT policies and procedures related to their job activities.	8	67
53	Ensure administrative personnel with cyber security responsibilities subscribe to one or more cyber security advisory services to receive up-to-date information on new cyber threats, attacks, exploits, and vulnerabilities.	8	68

Appendix C – Effective practices summary

54	Ensure that all computer-based devices and equipment undergo an initial deployment review to ensure appropriate system hardening is performed and the system configuration is in alignment with security requirements and policies.	8	69
55	Use passive media for the transfer of sensitive information; employ strong encryption with a complex shared key to secure the information; ensure that the media is either stored or destroyed in an adequate manner once the transfer has occurred.	8	70
56	Prior to loading or copying information/files/data onto a critical system or CDA, perform an anti-virus scan of the media and its contents on a separate system designated and configured for that purpose.	8	73
57	Where possible, use passive media when moving information between CDAs or between untrusted computers and CDAs.	8	73
58	Do not connect an unknown USB storage device to a critical system or CDA. It is recommended to purchase a set of low-functionality flash/thumb drives, label them for exclusive CDA use, and perform full sanitization and anti-malware scanning prior to using them with any CDAs.	8	73
59	Clearly mark and label active media devices assigned for use on critical systems/CDAs; implement reasonable positive-control measures to reduce the risk of intentional or accidental cross-contamination from unauthorized media.	8	74
60	Never connect untrusted portable digital devices to CDAs via USB without first running an AV scan on their file system by connecting them to a separate computer designated and configured for this purpose.	8	75
61	Never insert untrusted portable media into the media slots on printers connected to CDAs via USB, or shared by CDAs via a common LAN, unless the media has previously been AV scanned on a separate system.	8	75
62	Make use of cryptographic hash values to verify the integrity of files; generate (on a separate system) hash codes for files being exchanged with other parties, regardless of the files' contents/type.	8	76

63	Restrict portable computers/devices used in support of CDAs or critical systems to the NPR facility. Only connect those portable computers to critical systems/CDAs and isolated LANs within the NPR facility and never use those portable computers to access any site/server/system on the Internet.	8	77
64	Protect BUS/LAN-based smart instrumentation systems using appropriate measures such as physical means (locked enclosures, sealed conduits, surveillance, alarms, port blocking, anti-tamper, configuration tool control) and logical means (hardening, passwords).	10	81
65	Control access to all devices used for calibration and configuration, issue them only when needed and only to authorized personnel, secure them when not being used and have a second party confirm all changes made to calibration settings are correct and as approved.	10	82
66	Keep CDAs on their own isolated LAN or LAN segment.	10	83
67	Protect isolated Ethernet based instrumentation systems using appropriate measures such as: physical means (locked enclosures, sealed conduits, surveillance, alarms, port blocking, anti-tamper, configuration tool control) and logical means (hardening, passwords).	10	84
68	Prohibit the use of wireless instrumentation technologies in reactor safety applications.	10	85
69	Enable and utilize the security mechanisms available with wireless instrumentation standards.	10	86
70	Restrict the use of ZigBee wireless technology to non-reactor (e.g., facility automation) applications.	10	87
71	Confirm and validate that the configuration and settings of CDAs, digital devices and instruments are correct as part of reactor pre-operational checks.	10	90
72	Avoid dependency on software-based devices as the primary or sole means for initiating a reactor safety function or critical reactor operational/monitoring function. Analog/hard-wired circuitry is always preferable for reactor safety functions.	11	93

73	Restrict access to configuration settings on all CDAs using either physical or logical measures and strictly limit the number of personnel who are authorized to make configuration changes. If a portable digital device is used to make configuration changes to CDAs then limit and control access to the portable digital device and to vendor-supplied configuration software.	11	97
74	Ensure that the malfunction or mis-operation of a CDA or digital system cannot interfere with or block the hard-wired reactor safety shutdown functions.	11	99
75	Reactor safety CDAs should be isolated and physically secured and that maintenance, administration and configuration access would be monitored and strictly controlled through a combination of physical measures and integral protective measures.	11	100
76	Where PLCs or other types of digital devices employ a physical key to enable logic modifications (to be put into program mode) the key should be kept secure and anti-tamper measures should be used to detect unauthorized access to the PLC equipment.	11	100
77	Where possible, employ some form of HIDS that blocks unauthorized manipulation of the operating system settings and security functions and prevents unauthorized software from being allowed to execute (whitelisting).	11	101
78	Ensure adequate CDA cyber security and proper use of portable media.	11	104
79	Review facility digital design to ensure that current and planned digital upgrades will never cause a blocking of reactor SCRAM functionality.	11	104
80	Isolate CDAs that perform essential reactor safety and operational functions onto a separate LAN segment where possible.	11	106
81	Always include cyber security testing (or proof of such testing) as a requirement in procurements. For contracted software development this should include requiring the developer follow secure coding practices and perform the following: • Peer code reviews • Static code analysis • Vulnerability scanning	11	107

	• Known vulnerability testing • Secure language/library selection		
82	Develop a trusted vendor program restricting procurement of devices and software to only pre-approved vendors or from vendors who meet the appropriate qualifications and requirements.	11	108
83	When applying ANY digital/computer technology, ensure that a malfunction (accidental or malicious) of that technology (all or part) cannot prevent/block the reactor safety system from performing a SCRAM. Ensure that reactor operators have a diverse means of seeing the current values of essential reactor operating parameters so that a malfunction (accidental or malicious) in any one device/subsystem cannot blind the reactor operator to the true value of any of those reactor operating/safety parameters.	11	110